The vulnerability to Online Scamming

in contemporary Tongan Society

Ko e laveangofua ‘i he Ngaue Kākā ‘o e Naluopē

‘i he Sosaieti Tonga lolotonga

A thesis

submitted in fulfilment

of the requirements for the degree

of

Doctor of Philosophy in Computer Science

at

The University of Waikato

by

SIUTA LAULAUPEA‘ALU

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

2022

DEDICATION

This thesis is dedicated to:

My beloved mother

Leotisia Heilāpoli Laulaupeaʻalu (RIP)

and

My beloved father

ʻUsaia Vāvālafo Siuta Laulaupeaʻalu (RIP)

DECLARATION

Except where otherwise indicated
this thesis is my own work.

_____

Siuta Laulaupea‘alu

December 2022

ABSTRACT

This research explores the cybersecurity vulnerabilities of Tongan people to the rapid growth of Information, Communication and Technology (ICT). A research conducted by Laulaupea‘alu and Keegan in 2016 revealed that Tongan people were vulnerable to the influence of rapid ICT development (Laulaupea‘alu and Keegan, 2016). The cybersecurity vulnerabilities that were identified among the Tongan people in 2016 assisted in informing this research, which is to investigate the current susceptibilities in contemporary Tongan society. The aim of this research is to investigate the reasons why Tongans are vulnerable to ICT development specifically Online Scamming (OS) and find possible solutions to mitigate these susceptibilities. This research is the first to explore and narrow the scope to focus specifically on OS in Tonga. This research also focuses on the technical features of cybersecurity and then extends it to cover the cultural practices that would make Tongan people more susceptible to online scamming.

Laulaupea‘alu and Keegan (2019) directly conveyed these cybersecurity susceptibilities to the Government of Tonga (GoT) in 2018. This report confirmed that the actual position of cybersecurity in Tonga was that at least 73 percent of the organisations were vulnerable to cybercrime and cyberattacks. These organisations were victims of malicious software, spam, unauthorized access, social engineering, ransomware, data theft/data loss, stolen account, and other types of cybercrimes. This report also provided eleven (11) recommendations and suggested to the GoT to deploy these cybersecurity prevention and awareness features to assist in slowing down the issues of cyberattacks in Tonga.

One of the modern ICT accomplishments in Tonga was the installation of fibre-optic cable in 2013. Again, Laulaupea'alu and Keegan (2018) warned Tongans about the issue of succeeding in the fast internet speed of fibre-optic cable. The “high speed internet brings opportunities such as jobs and business but it also brings malicious cyber actors who can target victims in the nation” (p. 255). Drawn by the awareness of ICT issues that may arise and could lead to a stage where is unable to control, this research is undertaken to identify the root cause of these vulnerabilities, further looking for cybersecurity issues that are currently incurred and to discover appropriate defensive tools to counter these vulnerabilities.

The COVID-19 pandemic disrupted and became a major obstacle to this research. Due to border restrictions, there was no opportunity to travel to Tonga for data collection. To solve these issues, *e-fanongonongo tokoto* (e-ft) methodology was adopted to challenge the worldwide issues of COVID-19. The implementation of e-ft enabled effective communication from Hamilton to the survey participants in Tonga. E-mail, Facebook, Messenger and Zoom are the communication methods deployed by e-ft to communicate and collect data from one hundred and thirty-nine (139) participants ranging from 16 to 70 years of age. Participants were selected from government ministries, organisations, boards, businesses and ICT grassroots computer users from all five main regions of Tonga (Tongatapu, Vava‘u, Ha‘apai, ‘Eua and Ongo Niua). Although the e-ft process encountered many obstacles in collecting data from the survey participants, it was able to generate responses and data that have been analysed in this research.

Findings of this research reveal that Tonga is vulnerable to ICT development, and Tongan people are victims of cyberattacks due to the impact of rapid ICT development. These vulnerabilities relate to cybersecurity technical weaknesses, human behaviours, culture and personal beliefs of Tongans. This research also indicated that the people’s vulnerabilities were caused by five main elements: *greed, romance/love/empathy, lack of cybersecurity training, lack of ICT knowledge and unwillingness to report to authorities*. These vulnerabilities have resulted in the loss of credential information and the loss of money to cybercriminals from the people of Tonga.

Participants who took part in this research suggested powerful and long-term strategic plans to empower the prevention and awareness of Tongan people toward the impact of rapid ICT development.

ACKNOWLEDGEMENTS

Mou mavava ki he ʻOtua ē, ʻA e ngaahi fonua kotoa pē. Tauhi ʻa Sihova ʻaki ʻa e fiefia: Hū ki hono ʻao mo e kaikaila. ʻĒ, ke mou ʻilo muʻa ko Sihova pē ko e ʻOtua: Ko ia naʻa ne ngaohi kitaua, Pea ko kitaua ʻoku ʻoʻona; ʻIo, ko e kakai ʻaʻana, Ko e sipi ʻoku ne fafanga. Mou hū hono ngaahi matapā he fakafetaʻi, Hū hono ngaahi lotoʻā mo hono hivaʻi: ʻIo, mou sani pē ia, Fakamālō ki hono huafa. He ʻoku lelei ʻa Sihova; ʻOku taʻengata ʻene ʻaloʻofa; Pea tuʻu maʻu ʻene fuakava; Ki he toʻutangata mo e toʻutangata (Saame 100:1 - 5).

Shout for joy to the Lord, all the earth. Worship the Lord with gladness; come before him with joyful songs. Know that the Lord is God. It is he who made us, we are his people, the sheep of his pasture. Enter his gates with thanksgiving and his courts with praise; give thanks to him and praise his name. For the Lord is good and his love endures forever; his faithfulness continues through all generations (Psalm 100:1 - 5).

This research could not be accomplished without the close cooperation of the associated entities. Because of the combined efforts of all entities, it is highly praised for all the services contributed to this research. There are not enough words to say *maloo ʻaupito* (thank you) to all the members who offered their time, money and ideas to this research. Without your assistance, achieving the purpose of this research may have been impossible. Thank you so much for the assistance. *Mālō ʻaupito e tokoni*.

A heartfelt gratitude to the UoW for allowing the opportunity to enroll in this study program. All the resources provided were extremely valuable and I am unable to describe how precious, great and helpful these resources have been. It was the first time to experience the most efficient, productive, effective, powerful and economical resources provided by the university. The climax of the assistance reflects on the financial assistance offered by UoW through a three years scholarship to finance the costs involved. It was a great blessing for my family, and

I could not describe the great memorable moment we enjoyed. The financial aid offered met the family's desperate needs and became surplus and beyond.

A sincere salutation to my project supervisors' team – my primary supervisor, Associate Professor Te Taka Keegan and the other supervisors – Associate Professor David Nichols and Dr. Vimal Kumar. Your wisdom and knowledge steered me to choose the right pathway to walk. You guided me about the curbs ahead to step aside. You first recognised potential threats that lie ahead and reminded me of where they were located and directed me in the appropriate approach to address these threats. Your guidance was akin to a blind or low vision person that always requires someone to hold my hands. You took full responsibility to hold my hands and directed me to the final destination.

Your doors, emails and mobile phones were always 24/7 opened to walk inside, contact, or ask questions at any time. You never decline, deny, refuse or reject personal or academic requests from me. Your positive responses reminded me that you valued me and enforced me to keep motivated and confident and to show you that I also valued you. Without your contribution, this study may not accomplish and reach the end. All your support were valuable to guide and reach the end of the academic journey.

Achieving such a high level of education is a key milestone to write in our family's history. In addition, it will also be an important model for the family to follow in my footsteps, no matter of the circumstances (ages/ time/ money/ family), but achievement always counts. That would not have happened without your full assistance and robust support from UoW.

The milestone achieved by this research was made possible with the Government of Tonga's (GoT's) approval to conduct this research. An epic occasion to praise the government courtesy of providing their permission. Despite various changes due to the global crisis of COVID-19, the government still agreed to issue a second permit to conduct this research without visiting Tonga. The original approval is to a face-to-face interview with the survey participants. The second approval permission agreed to an online survey. As such, I am very grateful to the GoT and members who worked together to obtain these approval permissions. Again, there

are not enough words to praise the GoT and their related members for all your assistance. Without your help, this study would not have been accomplished.

The main key element of this research was the survey participants. These people carried out the core responsibilities and they showed their willingness to support. Without their support, this research is not yet completed. To all the survey participants from all the main five nations of Tonga, (Ongo Niua, Vava‘u, Ha‘apai, ‘Eua and Tongatapu), thank you very much for all the efforts and support that you offered.

There are a lot of people who contributed to this research. I am not keen to put all the names on this section. If I forget to say thank you to one or two names, they are going to blame me for missing their names. So, it is safer not to reveal names in case it does not all show up and then complain to me. In general, I would like to say thank you very much to all the supporters and all the people that commit their time to contribute to this research.

The most precious jewel of my life is a faithful, hardworking, loyal, and adoring wife. A loyal salute and honour to embrace and show how grateful she is. A wife who is enriched with the qualities of love, honesty, respect, support, share, listen, communication and appreciation. As she gained all these attributes, *all the messes turned into messages and the trials transformed into triumphs.* It was not an easy journey since the first day, but she had been close by my side to honour full support and make this dream become true. Despite the highs and lows of this long journey, she put them aside and looked ahead and stepped forward. My wife and my family are the key fundamental personnel for the achievement of this research project and there are not enough appreciative words to honour your complimentary assistance. *Mālō ‘aupito e tokoni ‘a hoku hoa ‘ofa‘anga, Valeti, pea pehē foki ki he‘eku fānau mo e fālmili/ kotoa. Fakamālō atu he ngaahi tokoni kotoa. Ke ‘a e ‘Otua ke ne foaki atu ha ivi mo ha tokoni kiate kimoutolu kotoa lolotonga ‘etau fononga me i Taimi ki ‘Itaniti.*

ACRONYMS

ARF	Australia Rugby Football
CIA	Confidentiality Integrity Availability
CROW	Cybersecurity Researchers of Waikato
FIU	Financial Intelligence Unit
FM	Facebook Messenger
FWC	Free Wesleyan Church
GM	Good Samaritans
GDP	Gross Domestic Product
HBIU	Home Based Internet Users
HSC	Hawaiki Submarine Cable
ICT	Information Communication Technology
IDL	International Date Line
IIU	Innocent Internet Users
IRS	Internal Revenue Service
Kms	Kilometres
LDS	Latter Day Saints of Jesus Christ
LRS	Literature Review Section
MMT	Mate ma‘a Tonga
ML	Machine Learning
MMT	Mate Ma’a Tonga
MRF	Microwave Radio Frequency
NCF	National Cybersecurity Framework

NCS	National Cybersecurity Strategy
NHBIU	Non-Home-Based Internet Users
OB	Online Banking
ORS	Online Romance Scam
OS	Online Scamming
OTP	One Time Password
PM	Prime Minister
PMO	Prime Minister Office
PoG	People of God
RBF	Reserve Bank of Fiji
RSE	Recognised Seasonal Employer
SARS	Severe Acute Respiratory Syndrome
SCCN	Southern Cross Cable Network
SDAC	Seventh Day Adventist Church
SoR	Sea of Red
TDB	Tonga Development Bank
TCM	Tin-Can-Mail
TIs	Tongan Innocents
TkT	Tongan-kills-Tongan
UMIC	Upper Middle Income Country
UoW	University of Waikato
USP	University of South Pacific
WHO	World Health Organisation

TABLES OF CONTENTS

Table of Figures

List of Figures

CHAPTER ONE

1. INTRODUCTION

ICT proliferates in the South Pacific Islands (SPI) and most of the SPI have converted from satellite network to modern fibre-optic cable. Fibre-optic cable network facilitates ICT developments and exposes the SPI globally. Fiji was one of the leading island nations to connect to the global submarine fibre-optic cable network in 2000 (Hogeveen, 2020). Tonga was the second nation to follow Fiji to upgrade their ICT system and to connect to fibre-optic cable in August 2013 (The World Bank, 2013b), then followed by the Republic of Vanuatu in early 2014 (Fintel, n.d.). According to RNZ (2018), American Samoa was also connected to a Hawaiki global submarine fibre-optic cable network in April 2018. The Cook Islands are reportedly working towards the installation process and RNZ (2020) confirms that the Manatua submarine fibre-optic is scheduled to start in May 2020. The Manatua cable is also planned to connect other islands of Rarotonga, Apia in Samoa, Tahiti, Bora Bora (French Polynesia) and Niue.

Since the conversion from satellite network to fibre-optic cable, there has been a substantial increase in the number of internet users in the SPI. For example, the number of internet users in Fiji has risen from 1.5% of the population in 2000 to approximately 46% in 2016. Likewise in Tonga the penetration rate has increased from 2.4% in 2000 to 46.6% in 2016. In 2000, the number of internet users in Tonga was 2,383 which is 2.4 percent of the total population (97,898). In 2016, the penetration rate has increased to 46.6 percent in which 49,822 out of 106,915 people in Tonga were able to access to the internet (Internet Live Stats, 2016).

1.1. ICT development in Tonga

A report from Kalvin Bahia (2018) states that mobile internet connectivity in Tonga increased 57.8% from 2014 to 2017. Digicel Tonga (2018), one of the domestic Internet Service Providers (ISP), celebrated the achievement of $4G^{+}$ services throughout the Kingdom in November 2018. Another confirmation report from Budde Communication (2019) confirms that the 4G LTE network was live in Tonga at the end of 2018. Global Voices (2019) estimates the number of Facebook users in Tonga is around 62,000. From this figure, almost 58 percent of Tonga's total

population (106,915 people mentioned in the last paragraph) were able to access Facebook in 2019.

A USD 4.5 million (the equivalent of TOP 9 million) fund from World Bank for digital transformation and e-government projects in Tonga is ready to be implemented in 2020 fiscal year. (TOP is referred to *Tongan Pa'anga* or Tongan currency and the usual symbol is T$ for *pa'anga* (dollar) and ¢ for seniti (cent)). Construction of a new datacentre to store and back up data is a part of this multimillion-dollar project. In addition, Asian Development Bank (ADB) is ready to assign TOP 14 million for installation of new software program for Tonga's Ministry of Health and to provide relevant cybersecurity procedures to ensure data is well secured (Tonga Broadcasting Commission, 2019). Rachinger, Rauter, Müller, Vorraber, and Schirgi (2019) explain digital transformation as "the continuous interconnection of all business sectors and the actor-side adaptation to the requirements of the digital economy" (p. 1145). The proposed digital transformation in Tonga will link various organisations, businesses and individuals locally and globally. Encouraging foreign investment in Tonga is not the primary focus of the ICT transformation but rather to enable greater capacity for E-learning, E-entertainment, and E-commerce service delivery (Petelo, 2017).

To ensure digital transformation and e-government services are safely outreached to Tongan citizens (including remote islands), more secured websites to facilitate access to government and business online services. According to CGI Security (2018), secured websites ensure relative components are patched and always updated. Major security components are Web Server (Apache), Web Application Server (Weblogic, Websphere and Tomcat), Database Server (Microsoft, Oracle, MySQL and SQL Server), Web Applications (Python, PHP, Java etc) and Proxy Server (Squid and Apache). Tonga's e-government project requires the above-mentioned cybersecurity components to secure websites and other significant digital mechanisms.

Senthilkumar, Gitanjali, Monika, and Monisha (2020) raise the following warning regarding a proliferation of websites.

> "*As the number of online websites increases, the chance of fraudulence also increases gradually*" (p. 414).

The digital conversion required to establish E-government websites in Tonga will require several resources to be developed. This could make it vulnerable to exploitation by scammers. The chance of future fraudulent acts warned by Senthilkumar et al. (2020) can be narrowed by deploying the security components discussed by CGI Security (2018) plus the inclusion of other cybersecurity procedures.

Since the major ICT transfiguration in 2013, the conversion from satellite network to the Southern Cross submarine fibre-optic cable connected from Fiji to Tonga, a new arena of cybercriminals has emerged throughout the entire Kingdom of Tonga. A former Deputy Prime Minister of Tonga, Hon. Siaosi Sovaleni mentioned that "Tonga have developed significantly over the years but the vulnerabilities to ICT related incidents also increased" (Government of Tonga, 2016). Awareness and prevention programs were prepared by the GoT to mitigate the ICT vulnerabilities and the growing effects of cybercrimes.

Figure 1: Professor Bruce Clarkson and Hon Siaosi Sovaleni

Source: (The University of Waikato, 2017)

As part of the awareness and prevention programs, a Memorandum of Understanding (MoU) was signed by Professor Bruce Clarkson, Deputy Vice-Chancellor Research, UoW and former Deputy Prime Minister of Tonga, Hon Siaosi Sovaleni from the GoT (see *Figure 1*) in May 2017. The MoU opened the door for the GoT to collaborate with the Cybersecurity Researchers of Waikato

(CROW) laboratory and to extend more research and learning opportunities specifically in the cybersecurity field.

According to the The University of Waikato (2017), this work builds on one of the Tongan students who recently graduated with a Master in Cybersecurity. A new student from Tonga was offered a scholarship under the MoU agreement to study for a Master of Cybercrime Security at the UoW in 2018. Four officials from the GoT attended the annual New Zealand Cyber Security Challenge (NZCSC) Event hosted by CROW, conducted in the UoW in 2018. The new knowledge and experience gained by these officials during the Cyber Security challenges are to be returned and utilised in Tonga (The University of Waikato, 2017).

1.2. Impacts of ICT development

Like other SPI nations, Tonga had experienced major issues of satellite network communication; the high charge, limited bandwidth and slow speed satellite network services (The World Bank, 2013a). The introduction of new fibre-optic cable in 2013 facilitated both internal and external ICT communication with the government ministries, banks, businesses, churches, hospitals and citizens. Issues associated with the old satellite network have been eliminated by the thriving fibre-optic connectivity. Fast internet speed delivers diverse connectivity paths locally and internationally. For example, doctors from the main hospital in the capital city Tongatapu can now communicate with their colleagues on remote islands. Video calls can be made to overseas specialists concerning complicated or urgent cases. Complicated services such as urgent surgeries link via video call to overseas experts to direct and assist local doctors. Growers and farmers can order goods online. No need to travel overseas but to order goods by face-to-face conversation with overseas buyers (The World Bank, 2013a).

Educational officials from the head office in Tongatapu link with the outer islands' students/teachers to conduct the normal daily basis training programmes for teachers. Tertiary students' online video tutorials facilitate communication through face-to-face with overseas lecturers and students can raise educational issues. Fast speed internet assists greatly with downloading resource material and uploading assignments. High gigabyte capacity supports saving of academic files online (cloud computing) (The World Bank, 2013a). Tonga Development Bank 'Ave

Pa‘anga Pau’ Online Banking services with the assistance of mobile phones take a few minutes to deposit money from overseas and then can be withdrawn by a family member in Tonga after a few minutes (Tonga Development Bank, 2016)

Indigenous Tongans, in particular the elderly, who have limited-access-knowledge of the internet, mobile phones, tablets, and computers, are assisted by younger family members to make video calls or to convey messages to immediate families overseas. The face-to-face video call has not only given them a sense of joy to see their family overseas, but it is also an opportunity for the older generation to look at the outside world from the outer islands or the sea or the farm or inside a house. Communities’ halls are equipped with TV screens and are open-free for the community to watch overseas news and sports.

A wake-up call for Tongans occurred in 2019 after a violent threat was posted on Facebook by a fake unknown author. The post appeared on Facebook in 2019 but is no longer occurred. The discourteous threat was directed at the King of Tonga’s family. Tongan officials led by Tongan Attorney General met with Facebook authorities in Australia to discuss and investigate the unknown author. A source from RNZ (2019b) that the GoT will step in to put an end to disrespectful, discourteous and abhorrent behaviours being practised on Facebook. The GoT is expected to announce soon the result of investigation into the threats made in the post. New Bills passed by GoT provide means of policing social media (RNZ, 2019b).

The fake Facebook post directed to the King of Tonga highlights important current values of Tongan culture and customs. The core-values or golden pillars of Tongan culture are *faka‘apa‘apa* (respect), *lototō* (humility and generosity), *tauhi-va* (loyalty and commitment) *mamahi‘ime‘a* (sense of responsibility) and *‘ofa* (love). In this case, there was no sign of respect, humility, loyalty, sense of responsibility or love by the way this unknown author freely expressed his or her personal views. In this case indigenous Tongans and the leaders in Government were greatly perturbed and upset by the disloyalty shown towards the King. By making this threat the core values of Tonga have been attacked.

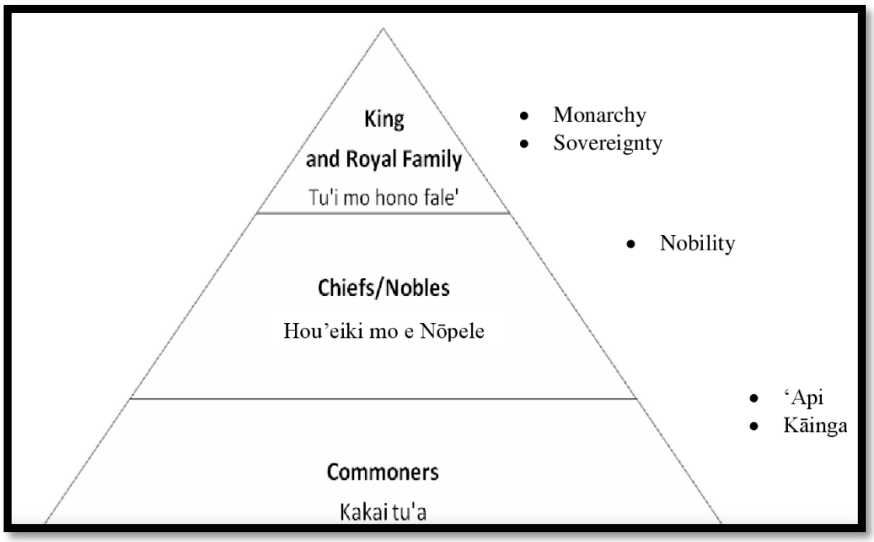


Figure 2: Tongan hierarchy triad

Source: (Teisina, 2011)

The King of Tonga retains the highest power in the nation and is the only indigenous monarchy in Oceania. There are three main classifications of people in Tongan ways of living. The King rests at the top of the hierarchy triad, the nobles at the centre and the commoners always remain at the bottom (see *Figure 2*). As is customary, the commoners sustain the *fatongia* (roles) to *tauhi* (look after) the 33 traditional nobles and as well as the king. In the middle of the triad, the nobles keep the *fatongia* to the king and the king remains as the King. The hierarchical division aims to denote the supreme power of the King of Tonga from the nobles and commoners.

Figure 3: Shortening of Tongan words

Source: (Folaumoetu‘i, 2020).

Figure 3 represents an informal text posted on Facebook on 03/03/2020. The Facebook poster, Folaumoetu'i (2020), is requested to Facebook users to provide a phone number of a friend.

TeAra (2015) states that many Tongans believe that without their language, people lose their identity. Indeed, theoretically, a real Tongan speaks, reads, writes and understands Tongan language. Therefore, when the following Facebook post is seen it can be said to have not upheld Tongan language standards. It includes incomplete sentences, word abbreviations and lack of appropriate language symbols leading to a sentence which is grammatically incorrect and nonsensical.

The nature of this post signifies multiple errors that remind Tongan officials about the importance of sustaining the structure of indigenous language. Freedom of expressing speech and thought is permitted but there are ways to expose formal writing. To maintain the indigenous language, Tongan officials together with the Ministry of Education are to set strategies commencing from Primary school to enforce formal writing when students are at the early ages. This is an opportunity for the younger generations to grow up with an appreciation and respect for the Tongan language.

To convert the post to a grammatical and formal Tongan language this is how it should be written: *'Oku 'ilo'i 'e ha taha ha fika telefoni 'a Tevita Vuki? Iceman, kataki tuku'i mai 'a e fika telephoni* which translates into English: *Is there anyone who knows Tevita Vuki's phone number? Iceman, if you know the phone number, please can I have it.*

There are shortfalls in the Facebook post in *Figure 3*. These are some of the corrections that this sentence requires:

- The sentence should be divide into two sentences to clarify that there are two main messages in this post. The first part is a question to all Facebook individuals to provide a phone number. The second part specifically asked one individual to provide the phone number.
- The inclusion of the word(s) 'Oku (Is there) to classify the first part is a question. A question mark should also apply at the end of the sentence.
- Grammatical corrections involve the addition of apostrophes, question marks, capital letters, commas, and periods at the end of the sentences.
- No consonant stands alone like the letter 'h' (the second word in the text). It should have a vowel 'a' to form 'ha' (there). Only the vowels (a, e, i, o, u) can stand alone.

- Incomplete and shortening of words such as h, tha, fka and pH are formalised by adding more letters to complete these shorten words (ha, taha, fika and phone)

All the above-mentioned examples show the consequences of social media on Tongan language in breaking down the cultural relationships between commoners, nobles and the King.

Faka'apa'apa (respect), is one of the Tongan core-values, is deteriorated as masked internet users with false identities can freely access Facebook to post false personnel critiques or discredit other citizens. A lack of *faka'apa'apa a* is shown by the August 2019 false personal critiques directed to the King of Tonga (as discussed previously). As a result of this disrespect to the hereditary monarchy, a consultation between the GoT and Prime Minister's cabinet occurred to temporarily ban Tonga from Facebook (Advox, 2019). Although several critics from various sectors voiced displeasure about the proposed ban, the GoT showed the seriousness of expressing disrespect to the hereditary monarchy by entertaining consultation over the proposed ban.

Another issue has been discovered by the misuse of words that are uniquely for the King of Tonga and therefore not appropriate for commoners to use. As mentioned previously, Tongan language is divided into three main divisions of social level: a language for the king (as in the top of the hierarchy triad), nobles (middle), and the commoners at the bottom. (More details of the division of the Tongan language are summarised in Section 2:5:1).

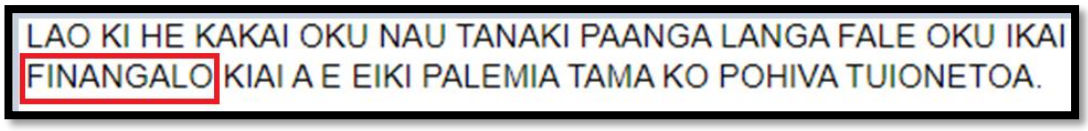


Figure 4: Word of King is misused for commoners

Source: (Facebook, 2020).

Tongan 1News, a Tongan Facebook media, posted a message on 12 November 2020. The message informs that the Tongan Prime Minister, Hon Pohiva Tui'onetoa, is not *finangalo* (in an agreement with), with the law concerning fundraising for building houses. The word *finangalo* (in an agreement with),

highlighted in red triangle in *Figure 4*, is specifically used for the king of Tonga. *Finangalo* can only be used in reference to the Will or wants or agreement of the King or God. Therefore, it is not in conformity with Tongan culture to use the word *finangalo* to refer to the agreement or will of any individual other than the King. Although the message is from the Prime Minister of Tonga, the Prime Minister is still from the commoners. High position in the Tongan community is not a virtuous reason to amend the structural position of the hierarchy triad.

1.3. COVID-19

The main reason for the inclusion of the COVID-19 topic in this section is because this research was overall affected by this global pandemic. The major fundamental action (implementation) of this thesis was to collect data from overseas (Tonga) but was incapable due to travel bans and border restrictions. That is why this topic is included in this chapter.

There is a COVID-19 topic in the Literature Review chapter which mainly focuses on recent discoveries and publications by several academic researchers. This section emphasis on the general overview of COVID-19, how the scammers cheat innocent citizens and some recent cybercriminal cases which occurred in the Asia-Pacific regions. The main contents of this section are the actual COVID-19 cybercriminal cases which are not yet published. The most interesting point is while the world is focused on finding antidotes to cure the global spread and high death rate of coronavirus, scammers deploy social media and fake websites as effective tools to deceive innocent internet users (IIU). With more citizens being locked down, isolated, under financial pressure and vulnerable, the COVID-19 environment is the perfect time for the scammers to take advantage and act fraudulently. Due to global concerns and the universal impact on family, health, economic, financial, education, culture, technology, communication, employment, social, religion, sport, tourism, transportation, travel, environment, politic, trade, store and many more impacts, COVID-19 sits at the top of the world's agenda - to fight against coronavirus.

The breakdown of the word COVID-19 is as follows: 'CO' represents 'Corona', 'VI' stands for 'Virus', 'D' for 'Disease' and '19' stands for the 'Year 2019' (Unicef, 2020) (p. 2). On 31 December 2019, unknown pneumonia discovered in

Wuhan China was reported to the World Health Organisation (WHO) Country Office. On 30 January 2020, it was declared to be a Public Health Emergency of International Concern. On 11 February 2020, WHO broadcasted a new name for this pandemic disease as COVID-19 (World Health Organization, 2020).

COVID-19, a pandemic and fast-growing mortality rate around the world, was initially emerged in November 2019 (Guardian, 2020). In the second week of March 2020 after three months from the emergence of this pandemic virus, Guardian (2020) reports about the growth and death – about 150 nations around the globe with 425,000 infected people and more than 18,000 deaths (Guardian, 2020). Today, 30 June 2021, the total number of confirmed cases is 181,488,102 and 3,931,204 deaths. The United States remained at the top of the world with 33,607,895 confirmed cases with 603,758 deaths. In New Zealand, the number of confirmed cases is 2,879 people with 2,824 recovered and 26 deaths as at 4th August, 2021 (World Meter, 2021).

In Auckland, New Zealand, in April 2020, several weeks into a nationwide lockdown, an individual found themselves a victim of fraud. According to Leahy (2020), the victim, Nitin Bhaskar from Mt Albert, made only one online bill payment and remained at home with his bank card and hardly went out to other places during the lockdown period. Bhaskar said the last time he used his card was in the local dairy and a pharmacy. The victim received a call from the bank to enquire about four unauthorised petrol transactions as petrol transactions as it was rare to purchase petrol from different gas stations within 30 minutes. The victim had no idea when and how this scam happened. ANZ immediately responded and closed the bank account. New Zealand Netsafe CEO said that “scams are up about 10 per cent on average at the moment and about 10 percent of our scam reports are linked to Covid-19" (Leahy, 2020).

Laulaupea‘alu (2021) also discusses the effects of COVID-19 on the people of New Zealand and the SPI. During the level 4 lockdown in Aotearoa in early 2020, “local Kiwis were confused as to what sort of things to prioritise – to purchase food first, or to buy essential goods such as heaters, or to purchase medical supplies” (p. 118). A chartered flight was booked to return Tongan citizens from Fiji in June 2020 but was cancelled due to new confirmed COVID-19 cases in Fiji during this time.

Losing hope of returning home for essential workers (more than 1,500 from the South Pacific Islands) who were booked to return to their respective islands in May 2020. As a result of this cancellation, some of the essential workers were suffered from depression and anxiety (Laulaupea‘alu, 2021).

In early April 2020, Tangata Pasifika (2020), a New Zealand TV and radio live show program for the Pacific citizens in Aotearoa, warned the Pacific citizens to stay vigilant of COVID-19 scams. The interviewee explains that a message on Facebook asked the interviewee’s friend to donate money for a child in a hospital. Details were not clear as to which Pacific Island the patient came from or whether the patient is from Samoa or Tonga or any of the SPI nations. The interviewee also warns about the regular tactics used by scammers such as email phishing, open infected attachment, and fake websites. During the lockdown period internet users were warned to double-check the legitimacy of demands from vendors with regard to online bill payments (Tangata Pasifika, 2020).

In mid-March 2020, Interpol (2020) clarified recent cybercriminal cases related to COVID-19. As demand for medical supplies is high, cybercriminals set up online fake shop-websites with the promise to deliver masks and health supplies to innocent citizens, but no supplies were delivered. Other cybercriminals pretending to be health officials advise families to donate for medical payment of close relatives yet no patients in the family were admitted to a hospital. Other cases involved email phishing whereby scammers pretended to be from legitimate health services seeking payment details, personal credentials or offering enticement to open a malware attachment. Interpol (2020) moved to protect users by promptly closing false accounts sought up by cybercriminals.

1.4. Cybersecurity in Tonga

An outline of the actual position of cybersecurity in Tonga is described in the following paragraphs. According to S. Laulaupea'alu and T. T. Keegan (2018), cybersecurity, either in Tonga or throughout the Pacific Islands, is referred to as “new topic” (p. 257). New topic means there are a lot of cybersecurity gaps to explore. One of the security gaps is the lack of cybersecurity experts. Due to the absence of cyber-experts to maintain the Confidentiality, Integrity, and Confidentiality model (CIA), cyber attackers get more opportunities to find

loopholes and then access into the ICT system to gain credentials and sensitive information (username, password, driver license, bank account number, medical record, and private information). Several tactics deployed by cyberattacks to exploit and gain sensitive information are phishing, malware, ransomware, denial of service, crypto jacking, a man in the middle and SQL injection (Fruhlinger, 2020).

Laulaupea'alu and Keegan (2019) provides additional evidence of an ATM scam that affected bank customers in Tonga and Fiji.

> "…..*that some Tongan customers of BSP bank have reissued new cards after their cards were blocked. This problem is known as an ATM scam, and it is believed that the problem initially started in Fiji and then spread over to Tonga. An announcement from the Tonga National Reserves Bank (TNRB) confirmed that the ATM scam was caused by criminal activities. Customers were affected by unauthorized transactions on their bank accounts*" (p. 187 – p. 188).

Regarding this scam, Fiji Sun (2015) confirmed that six overseas nationals were arrested in Fiji in December 2015 with over $10,000 money in cash and fake ATM cards found in their possession. A customer found a skimming device (including a tiny pinhole camera) had been secretly attached to an ATM machine in one of the BSP branches in Nadi. It is believed this camera was used to obtain PIN numbers in this particular scam.

Laulaupea'alu and Keegan (2019) hand-delivered updated physical reports to the Prime Minister's Office and various GoT ministries of Tonga in 2018. Electronic copies were also delivered to participants through emails and Facebooks to show the actual position of cybersecurity in Tonga.

> *The survey results reveal that at least 27 percent of the organisations have been victims of malicious software, 26 percent have been victims of Spam, 6 percent have been victims of Unauthorised Access, and 5 percent have been victims of Social Engineering. It also shows 3 percent have been victims of ransomware, 3 percent have been victims of data theft/data loss, 1 percent is bullying, 1 percent is a stolen account and 1 percent is for another type of crime. Only 17 percent of the organisations have not been victims of cyber threats and cybercrimes, 8 percent did not answer the*

> *question and 2 percent had difficulty in answering the question. In summary, at least 73 percent of Tonga's organisations are victims of cybercrimes and cyber threats* (p. 188).

As the actual status of cybersecurity in Tonga is 73 percent vulnerable to cybercrime and cyberattacks, Laulaupea'alu and Keegan (2019) provide recommendations to the GoT. The eleven recommendation points that were suggested to be deployed in Tonga's ICT system are:

- Penetration Testing (PT)
- Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP)
- Budget
- Cyber Insurance
- Cyber Security Experts
- Information Security Policy (ISP) & ISO
- Data Encryption
- Data Backup
- Two Factor Authentication (TFA)
- Password Renewal & Password Setting
- Database Consideration

Tonga CERT (Computer Emergency Response Team) is the first island in the SPI to become a member of APCERT (Internet Society, 2020). Tonga CERT is the first point of contact for cybersecurity issues. Main tasks include handling ICT cybercriminal cases such as hacking, computer virus, data leakage, and vulnerabilities in the ICT system. CERT also targets to provide safe ICT environment for Tongan citizens through intimate collaboration with investors to manage cyber-threats at a global platform. Additionally, the GoT has enacted their computer own act. According to Scott (2007), Tonga Computer Crimes Act 2003 "deals with computer offences such as illegal access, interfering with data, interfering with computer systems, illegal interception of data, and illegal devices" (p. 101).

In October 2016, the Chief Executive Officer (CEO) of Tonga's Ministry of Information and Communications revealed that there are additional requirements to upgrade the current legislation.

> "*Tonga currently has the Computer Crimes Act 2003….. additional regulations are required to combat cybercrime*" (RNZ, 2016).

The uploading of inappropriate video material and defamatory statements onto Facebook have caused such concern that GoT's Attorney General has submitted a draft regulation to parliament. The former Solicitor General of Tonga, 'Aminiasi Kefu has stated that the current issues of bank fraud, online deception and email spams should be incorporated into the current legislation (Kefu, 2011). In 2019, the GoT passed a new bill as a replacement to the 2003 legislation. The new Computer Crimes Bill 2019 contains 78 sections with five main parts: computer-offences, miscellaneous provisions, procedure powers, interpretation and computer-related offences (Government of Tonga, 2019).

A cyberattack caused one of the GoT's ministries to lose a large sum of money in 2016. Laulaupea'alu and Keegan (2019) have expressed concern about this cyberattack and the level of computer illiteracy in Tonga.

> The bogus email that happened in Tonga identified some of the real implications of the lack of IT knowledge of Tongan government representatives. These people are in the 'green tree' level and trusted within the community due to their education and job status. They deal with emails and gain experience with IT related works in their workplace every day but were still caught out by a relatively simple online scam. The 'firewood' level (dead tree or *'akau-momoa*) are obviously more susceptible due to their lack of IT understanding, which is likely to allow more opportunities for scammers. The fake email scam and the significant amount of money lost in this scam highlights that Tonga is vulnerable to cyber-attacks (p. 187).

Firewood (dead tree) sparks easily to produce fire. Green tree (living tree) is wet and hard to ignite a fire. 'Firewood level' is referred to computer illiterate citizens and the 'green tree level' is for the civil servants that are frequently working with computers in workplaces. Green tree level understands more about ICT than firewood level. Firewood level gets higher chances to trap in cybercriminal's bait due to unfamiliarity with official ICT transactions (e.g., emails) in workplaces. The bogus email scam which occurred in Tonga involved those at the 'green tree'

(computer literate) level, but this did not stop them falling victim to a simple cyberattack trick.

1.5. Motivation

Tonga belongs to the small island developing states (United Nations, 2014) (p. 150) with resource-less and limited cybersecurity knowledge to counteract cyberattacks. A developed nation similar to the United States, who has monetary power ("The United States was the richest developed country on Earth in 2019, with a total GDP of $21,433.23 billion") (Investopedia, 2021) (paragraph 3) is still suffering the financial consequences. Statista (2021) highlights the largest cybercrime loss in California was over US$621.4 million and US$415.8 million dollars in New York in 2020 (paragraph 1).

Tonga's cybersecurity status is majorly vulnerable ("73 percent") (Laulaupeaalu and Keegan, 2019) (p. 188) to cyberattacks. Due to vulnerabilities to cybercrime and cyberattack, this thesis aims to find the reasons why Tongan people are susceptible to the rapid growth of ICT development. This research intends to look at multiple areas to gain as much information as possible. The research areas deal with technical features of cybersecurity, human, cultural and the daily usages of the internet by Tongan citizens. At the end of this research, a report is to be presented to the GoT to show the cybersecurity status of the internet in Tonga.

From a cultural perspective, this report intends to revitalise the ancient formulae of Tongan ways of living. Especially, individuals who are reluctant to hear the advice of ICT professionals and older generations, this is a chance to deliver facts from academic and PhD research findings. It is also an opportunity to outreach the cybersecurity facts (project research findings) to minority communities. This would have enabled the general populace to benefit from this research, particularly those at the grassroots level. There is hope that the survey findings are to reach to indigenous citizens so that the *kau-ta'e'iloa* (unrecognised and lower-level citizens in the community) would come to understand the cybersecurity weaknesses (in terms of Tongan ways of living).

Much research has concentrated on the technical features of cybersecurity to provide defensive practices to counteract cyberattacks. According to Aldawood and Skinner (2018) some of the wildest growing corporate crime-fears no longer deal

with the exploitation of ICT systems. Cyber attackers have "focused on humans, a target considered to be the weakest link in every enterprise" (p. 62). An opportunity to investigate other cultural features apart from core-values. Tonga is known as "*ko e fonua lotu 'eni" or* "…this is a Christian nation..." (Niumeitolu, 2007) (p. 7) which is significant to examine the relationship of modern ICT to religious beliefs. *Ko e ngaahi fatongia* (the roles) of Tongans to the church are 'must' responsibilities and 'must' be fulfilled. Tofuaipangai and Camilleri (2016) state that "*Fatongia* is an essential part of being Tongan". *Fatongia* is an element of *fua kavenga 'a e Siasi* ("to carry the burden" of the church) (p. 62) which involves *misinale* (church donation), *li pa'anga kuata* (quarterly donation), *konifelenisi* (conference) and *fakaafe* (feast). Pressure for individuals to uphold these elements may lead to an individual's involvement in cybercrime as they seek to uphold the concept of *fua kavenga 'a e Siasi.*

To date, no research has been conducted in Tonga or other Pacific nations relating to cybercrime. This is the first time to conduct research in this area. As the nature of this research project is new, there is an intention that the conclusion of this research project will discover the actual vulnerabilities and complications of online scamming in Tonga.

1.6. Thesis statement

This research identifies guidelines for implementing heightened cybersecurity measures in Tonga and the South Pacific region. The investigations have two points of focus. The first determines and analyses the occurrence of cyber-events in Tonga. The second seeks to understand the factors peculiar to Tongan social norms and geographic settings that might affect generally accepted security measures in ways that make ICT systems in Tonga more susceptible to online malevolence. The research will address the following questions:

1. *How has rapid ICT deployment in Tonga influenced online vulnerabilities?*
2. *How is the incidence of malicious cyber-events in Tonga exacerbated by particular aspects of Tongan culture?*
3. *What strategies have been identified by the research to improve ICT security in Tonga?*

This investigation intends to:

- investigate cybersecurity awareness and perceptions in Tonga
- understand current Tongan cybersecurity capabilities
- identify the vulnerabilities of Tongans to internet frauds and online scamming
- identify opportunities to implement prevention and security measures in Tonga
- suggest guidelines and processes that can inform cyber-security strategy and policy

The scope of this research includes addressing the research void in Tonga and the wider South Pacific in terms of online malicious events. Further factors will be investigated that may be contributing elements to cyber vulnerability, for example, geographic isolation, religious beliefs, socio-economic conditions, and aspects of culture, tradition, and familial ties.

Cybersecurity awareness and prevention in Tonga is a priority driven by the prevalence and widespread consumption of digital technologies and the current design and deployment of e-Government, an initiative to digitalise government services so they are more accessible to citizens. Cybersecurity capabilities must be developed, and security measures applied to avoid cyber intrusions and to ensure ICT safety in Tonga.

1.7. Thesis outline

This thesis has seven (7) main chapters. Details of main contents of each chapter are outlined in ***Table 1*** below.

Table 1: Thesis Summary

Chapter	Description of Chapter
Chapter 1	**Introduction** The first chapter summarises the global growth of ICT and then discusses the wave of ICT transformation from developed nations to propagate the SPI. In the SPI, Tonga is one of the nations currently involved in the wave of ICT. The section is further divided into subsections to clarify the following points: ▪ rapid uptake and engagement by the general population of Tonga ▪ ICT development and uptake mean to the indigenous / minority/ under-resourced languages and cultures.

	▪ impact on oral traditions, tradition social structures, language and culture ▪ the general impacts of COVID-19 ▪ Cybersecurity in Tonga ▪ Personal Statement and Project rationale ▪ Thesis Statement ▪ Thesis Outline
Chapter 2	**Background** A precautionary Tongan proverb introduces this section about the readiness for the consequences of ICT development and cybersecurity vulnerabilities. A further discussion touches other areas such as ▪ The general overview of Tonga ▪ Social, culture, history, economic, religious and physical features of Tonga ▪ Tongan Language ▪ ICT Connectivity
Chapter 3	**Literature Review** This section summarises general overviews of different types of online scamming and cybersecurity criminal cases from around the world. While the discussion focuses on cybercriminal cases in developed states, the scope was then narrowed to focus on comparing cybercriminal cases with poor nations including SPI and Tonga. The literature review covered the discussion about cybercriminal cases in the developed states, developing and underdeveloped nations. The section is then extended to cover these areas: ▪ Description of online scamming ▪ Cybersecurity prevention and awareness methods ▪ Cybercrime in developing nations ▪ Cybersecurity in the South Pacific ▪ COVID-19 Scams
Chapter 4	**Methodology**

	In this section, a deployment of *e-fanongonongo tokoto* (e-ft) methodology to communicate with the survey participants to solve the COVID-19's issues. The *eft* is then theorised on how it is aligned to the original concept of e-ft. The e-ft is then put into practice to communicate and collect data from the survey participants in Tonga. The active methods to communicate and deliver survey questionnaires to the survey participants were emails, Facebook Messenger and Zoom. A further discussion on e-ft to reveal the major issues encountered during data collection. This means the deployment of e-ft had experienced highs and lows during the data collection period.
Chapter 5	**Data Analysis** This is one of the backbones and major parts of this thesis. It recapitulates the results of the survey findings by using numbers, tables, percentages, graphs, and texts to summarise the information gathered from the survey participants. The highlights of this chapter reflect on the ability to identify cybersecurity vulnerabilities in Tonga and the methods to assist in mitigating these vulnerabilities.
Chapter 6	**Discussion** The focal point of this section is about exploration, detailing, meaning, and theorising of the survey findings. It is an in-depth evaluation of the core cybersecurity vulnerabilities discovered in this research. Although there are many vulnerabilities encountered by the people of Tonga, there are high priority areas that are likely to cause serious impacts and it is required to prioritise and raise it up in this section. The highlight of this chapter is about the information collected or data collections discovered in the Data Analysis section aligned with the three main questions that guided this thesis.
Chapter 7	**Conclusion** This is the very last section of this thesis. A very short section but it concisely summarises the achievement of the thesis. The thesis concludes that Tonga is vulnerable to OS.

CHAPTER TWO

2. BACKGROUND

2.1 Introduction

To understand the factors influencing Tonga's vulnerability to cybercrime one must first understand the Tongan culture. The second thesis question in particular asks how culture, the environment, and religious beliefs can be influencing factors. Consequently, chapter two gives background on those aspects so that they can be considered when addressing the research questions.

Chapter Two consists of eleven (11) sub-sections. An introductory Tongan proverb provides metaphoric precautionary advice for Tongan people. There are two main themes of the proverb: preparedness and awareness. An overall warning for the people to follow the cybersecurity experts' advice and get ready for unintentional occasions in future. In the end of this chapter, a clear explanation is given regarding the significance and relationship of the Tongan proverb to the thesis topic.

The second subsection (Section 2.3) explains Tonga followed by the presence of other related indigenous features such as history, language, population, location, economics, culture and religion (i.e., from Section 2.4 – Section 2.11). The inclusion of these indigenous features is not only for cultural preservation but some of these features are fundamental elements in the survey questionnaires. Section 2.12 takes a summary of the whole chapter.

Summary of Chapter Two is detailed below:

- Section 2.2: Tongan Proverb
- Section 2.3: Tonga
- Section 2.4: History of Tonga
- Section 2.5: Language
- Section 2.6: Population Distribution of Tonga
- Section 2.7: Location and Isolation
- Section 2.8: Economics
- Section 2.9: ICT Connectivity
- Section 2.10: Tongan Culture

- Section 2.11: Church and Religious Belief
- Section 2.12: Chapter Summary

2.2 Tongan Proverb

A well-known Tongan proverb pronounces '*Tala kei 'i Kapa na'a ke tō ki Mala'* ("Tell it while still in Kapa"). 'Ahio (2018) interprets that the meaning of this proverb translates in Tongan as "*Ko e teuteu mo e fakatokanga ki ha faingata'a 'oku teu hoko mai he kaha'u*" (p. 80). Cocker (2013) provides another definition, "*Koe tokateu ki ha faingata'a 'e ala hoko he kaha'u*" (p1). Both interpretations from the authors, 'Ahio and Cocker, are synoptic in presenting an analogous view of vigilance, awareness, readiness and in-advance preparedness for challenges and dangers that lie ahead. A metaphorical interpretation of the main theme of '*Tala kei 'i Kapa na'a ke tō ki Mala'* can be transformed and applied to contemporary ICT in the field of cyberattacks and cybercrimes.

Rabone (1845) defines the meaning of the word *tala* as "to tell" (p. 189). Baker (1897) adds that another definition of *tala* is "to reply" or "to speak of" (p. 182). *Tala* (tell) simplifies action: to convey, deliver, notify and to pass on a message from one place to a precise destination/individual. An ancient communication method practised by Tongans to verbally *tala* or pass on a message from one *fale* (house) to the next *fale*.

Ofanoa, Percival, Huggard, and Buetow (2015) clarifies this type of communication was known as "*fanongonongo tokoto*" or "person-to-person contacts" (p. 335). *Tokoto* is to "lie down" or to "be lying down" (Baker, 1897) (p. 193). Rabone (1845) defines *fanongonongo* as to "promulgator, to publish, to noise" (p. 89). An individual, while lying down in bed inside a house, screamed to the next *fale* or neighbour to *tala* (convey) a message. The first message recipient or neighbour *tala* (passes) the same message to the next neighbour and so on until the message reaches the end of the village. *Fanongonongo tokoto* was practised in Tonga in ancient civilisation, without a telephone or internet or a body to deliver the message to reach the destination. Today, the concept of *fanongonongo tokoto* is very popular as a message is conveyed from a bed or room or house to expose to the outside world, assisted by ICT devices.

Kapa and *Mala* symbolise different meanings and memories. Both (*Kapa* and *Mala*) are two different islands in Vava'u, the second largest region in the Kingdom of Tonga. Also, *mala* refers to suffering the consequences, wages-of-sin, the outcome of disobedience and law-breaking. Tu'inukuafe (1992) explains that *mala* is a "misfortune for wrongdoing" (p. 188). Baker (1897) defines *mala* as a "foolishness" or "evil" (p. 150). The magnitudes of *mala* lead to *mala'ia*. Poltorak (2007) expounds that *mala'ia* is "bad luck" or "misfortune as the result or nemesis of wrongdoing" (p. 16).

Kapa is also known as a "Tin" (Baker, 1897) (p. 113) or a container. Earlier, *kapa* was reused by the people of Tonga for storing food and other valuable luxuries. Niuafo'ou Island is known as "Tin Can Island" (Bourdeix et al., 2011) (p. 35), located to the far North of Tonga, put letters in biscuit tins and kerosene cans as mailbags. Upon the arrival of a steamship, a native swimmer (see ***Figure 5***) carried the Tin-Can-Mail (TCM) to the offshore boat and carried back the inward mail respectively (FIP Postal, 2016) (p. 14), (J. Lewis, 1979) (FIP Postal, 2016; Lewis,1979).

Figure 5: TCM swimmer carrying mail from offshore steamship in 1930

Source: (FIP Postal, 2016)

TCM illustrates two imperative realities in an earlier time in Tonga. Firstly, the importance of the *kapa* for the ancient citizens was an essential instrument for

storage and carry of treasured luxuries. Secondly, TCM reminds the indigenous communication method to deliver messages (mails) from an isolated island to other parts of the world. Today, modern ICT takes a few seconds to connect to the outside world. But the TCM system used in Niuafo‘ou Island Tonga in 1930, takes longer to reach the destination.

A conversant story in Tonga about the legend of *Mala* and *Kapa* relates to the proverb ‘*Tala kei ‘i Kapa na‘a ke tō ki Mala’*. A *taula-tevolo* (brutal witchery or god-and-human) resided in *Mala* Island. The ordinary sea voyage to Neiafu, the capital of Vava‘u, came via *Kapa* the first island, then *Mala* the second island and then to Neiafu, the capital. Traditionally, the people of *Kapa* Island took responsibility for alerting new boats/sailors about the *taula-tevolo* on *Mala* Island. *Kapa* citizens beat the *kapa* (cans) to signal the sailors to wait, then came down to meet the new sailors and to offer advice about the *taula-tevolo* on *Mala* Island. The advice is either change the route to another longer route or to not make noises nor drop an anchor close to Mala ('Ahio, 2018), (Talakeikapa, 2018) (‘Ahio,2018; Talakeikapa, 2018).

Sailors who refused to listen to the advice from the people of *Kapa* and insisted on continuing the voyage through *Mala*, were trapped and killed by the *taula-tevolo*. A pre-warning from the people of *Kapa* to the new sailors to be aware of a ‘*taula-tevolo’* in *Mala* Island. Sailors are to make the right decision while in the safe zone of *Kapa* before reaching the death Territory of *Mala* Island. Making the right decision is subject to reaching Neiafu (destination) safely.

‘*Tala kei ‘i Kapa na‘a ke tō ki Mala’* is symbolic to this research as the general meaning of this Tongan proverb is to give precautionary advice. Failure to comply with the guidance of cybersecurity experts will mean there is no hope for a safety ICT environment in Tonga. Talakeikapa (2018) summarises the meaning of the proverb, like previous definitions in this chapter, is:

> *“……. to prepare in advance for the challenges that lie ahead.*
>
> *……. to warn someone or a group of people of the difficulties they may face in the future*” (Talakeikapa, 2018. paragraph 1).

The three main themes derived from this Tongan proverb are:

Be prepared: being prepared assists in the reduction of anxiety, risks, financial losses, and ready to defend. Brown (2000) says that "The best preparation for tomorrow is doing your best today" (Kelly Kuehn, 2019) (paragraph 6). An early prepare gives more chances to prepare well, knows the weaknesses and strengths of cyber-threats and understands the general overview of cybersecurity that needs to be prioritised.

A chance for the cybersecurity experts (either local or overseas), the holder of ICT knowledge, to share the ICT experience with the GoT and then pass the knowledge to newbie ICT users. Also, an opportunity for the GoT to take the basic cybersecurity preparation and awareness platform by alerting the people about the consequences of ICT.

Change direction and take the safe path: To change the direction from the original plan costs time, conflicts and losses. The advice of the experts/elderlies to change direction, comes from experiences, deliberately for the safety of the followers. Safety is the top priority. It is not too late to change the plan as the safe path leads to a safer future.

According to Gumbel (2020), a Vicar of Holy Trinity Brompton, London, and the pioneer of Alpha Course Study, there is always a chance to change direction if the original journey missed the right pathway. "No matter how long you have travelled in the wrong direction, you can always turn around" (Gumbel, 2020).

There is another chance: The alarm from the people of *Kapa* Island created by beating the *kapa* (tins) amplifies the chance of survival for the sailors (Tongan people). A clamp or trap in a net is not the end; there are several ways to free and get out of trouble. To be free yourself and get out of trouble, the advice of elderly/experts is noteworthy as these people get more life experiences and the followers (people) need to hear and take their advice.

A warning for the people of Tonga to be aware of the internet and ICT development. Beating the *kapa* to alert the people to be always prepared for unintentional interruptions. Failure to follow the instruction from ICT experts will lead to *mala* and danger. Although the cybersecurity development in Tonga is in the process of building up, whatever security advice from security experts is most relevant to be notified. Whenever unintentional attacks strike, the people (Tongans) already get a

fair understanding of possible defensive techniques to stabilise the attacks. It's a matter of readiness, self-reliance and attaining the ability to protect themselves from unintended attacks that may occur and cause harm to the people of Tonga.

An opportunity for the researcher and other cybersecurity experts, as the holders of cybersecurity knowledge, to hit the *kapa* as a loud bell in all the ears, to wake up, and to act, to protect the current and future generations before the '*taula-tevolo'* (problem or cyber-attackers) hold and control the Tongan people.

2.3 Tonga

Tonga, officially known as '*Pule'anga Fakatu'i 'o Tonga*' (The Kingdom of Tonga) or 'Friendly Islands' (Britannica, 2021) or 'A Polynesia Paradise' (Travel Guideline, 2011), was first discovered by Dutch navigators Willem Schouten and Jacob Le Maire in 1616 (Travel Guide, 2020). Another Dutch sailor, Captain Abel Janszoon Tasman, visited Tonga in 1643.

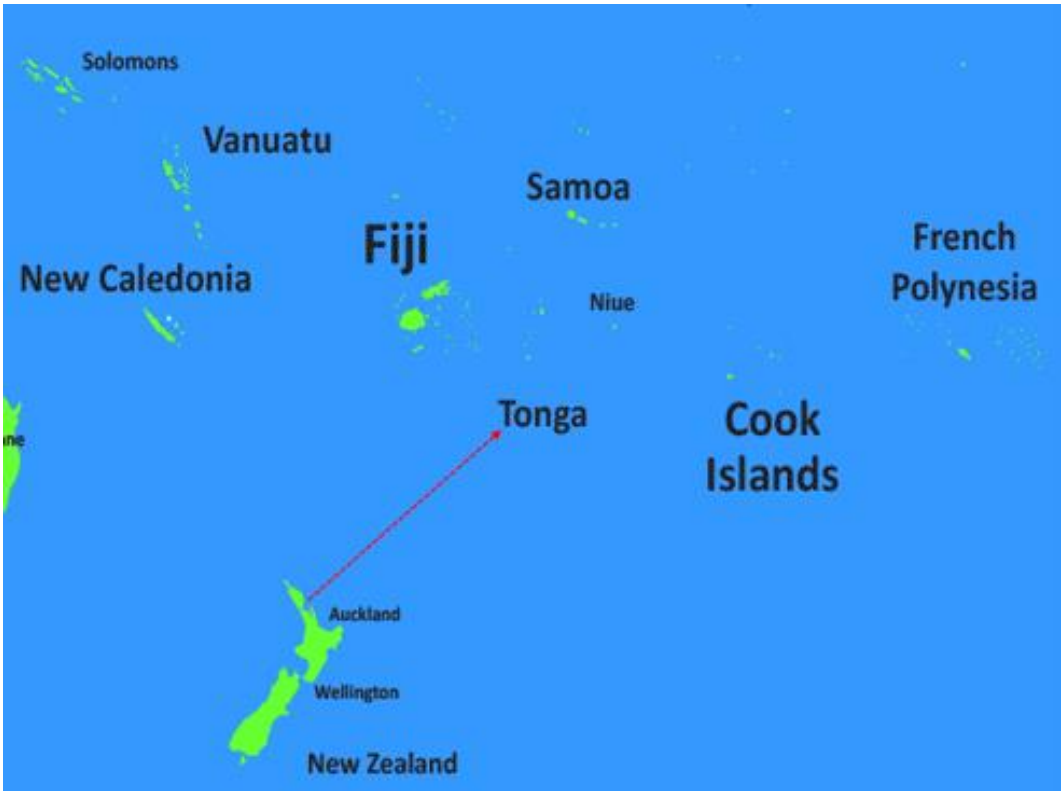


Figure 6: Map of New Zealand and Tonga

Source: (Thompson Memorials, 2015)

Tonga, located in the central Pacific (See *Figure 6)* with approximately 2,379 kilometres from New Zealand (air-travel distance of 1, 478 miles), takes only 3

hours flight from Auckland Airport, New Zealand to Fu'amotu Airport, Tonga (Distance, 2021).

As the main island of Tongatapu was an abundance of food, fresh water and replenishments, Tasman named this island as 'Amsterdam' (Society, 2020). In 1773 and 1777, an English mariner Captain James Cook visited the archipelago and was impressed by the warm hospitality of Tongans and gave the name 'The Friendly Islands' (British Library, 2018).

Figure 7: Map of Tonga

Source: (World Atlas, 2021)

Figure 7, the map of Tonga, shows all the five main divisions of Tonga: Tongatapu, Ha'apai, Vava'u, 'Eua, and Ongo Niua. In the map, an indication of three red circles reveals the three main regions (Tongatapu, Vava'u, and Ha'apai Group). All these three islands are the main centre of ICT development as they are fully connected to fibre-optic cable.

Travel Guide (2020) provides more information about Tonga which are as follows:

- Total Area: 748 km^2
- Language: Tongan and English
- Currency: Pa'anga (TOP)
- Capital: Nuku'alofa
- Population: 112,000 in 2005
- Religion: Christian
- Time: UTC + 13 hours (Universal Time Coordinated)

The Friendly Islands, a member of the United Nations and the Commonwealth, consists of 170 islands and is divided into five main provinces: Tongatapu, Vava'u, Ha'apai, 'Eua, and Ongo Niua. A constitutional monarchy ruled by Tupou VI who was crowned as the King of Tonga in March 2012. By tradition, the king is the ultimate power of the nation which has executive arms of government, the Privy Council, the Legislative Assembly, and the Cabinet. The King rules the nation, and the Prime Minister (PM) operates the government. The election of the PM is chosen by the 26 members of the Legislative Assembly. Then, the PM selects the cabinet members and submits to the King for final formal approval. The Legislative Assembly consists of 26 elected members, 17 members who are elected by the people and nine noble members voted by 33 nobles, to be their respective representatives. The PM is free to nominate four outside members from the Legislative Assembly to be in the cabinet (Commonwealth, 2020).

2.4 History of Tonga

In previous eras, Tongans revealed civilised life. Civilisation involves educational attainment so that cultural sustainability becomes more predominant to inherit and pass on from elderlies to the younger generations. Baker (1897) translates the word civilise into Tongan meaning as "*ke ako ke boto*" (p. 14) or to study to be *boto* ("wisdom, knowledge, skill, wise, knowing and discerning") (p. 26). Allen (2018)

states that civilisations are "accomplishments of knowledge, unthinkable apart from superior technical and artistic performance" (p. 246).

In 1773, the first arrival of Captain James Cook in Tonga, a man rowed in a canoe from the land to meet Cook's crews to offer a gift. Ferdon (1987) explains that:

> "One of the men in the first canoe to reach the ship off Tongatapu offered Cook a piece of kava root apparently as a gesture of friendship" (p. 55).

Kava is a plant; its roots and stem are used for drink and cultural activities. *Kava* represents the *fonua*, "the land, its people, and their traditions" (Tecun, 2017) (p. 7). The humbleness and willingness of the man to offer the *kava* represent the land, traditions and the overall people of Tonga. Turner (1986) explains more functionalities of *kava*. *Kava* (piper methysticum) liquid is "a beverage infused from the root of a pepper plant" (p. 203). Drinking kava is a form of ritual or ceremony found in the Pacific Islands such as Fiji, Samoa, Tonga, Futuna and Uvea (Turner, 1986).

Vaioleti (2006) provides another evidence of civilised life in Tonga before the arrival of Christianity in 1826.

> One must remember that Thomas arrived only in 1826 with education and the Christian ways of being, but Tonga had its civilised ways already, which the Christians' ways resembled.
>
> When the missionaries arrived, the Tongan ways of being were already in place, being at the same level of enlightenment as those brought by Christianity (p. 28).

2.4.1 Queen Elizabeth II's Coronation

In history, one of the most inherited memories of Tongans relates to the 1953 coronation of Queen Elizabeth II in the United Kingdom. The humbleness and the performance of Queen Salote, the late Queen of Tonga, during the coronation ceremony proved the ancient existence of civilisation in Tonga.

Salote Tupou III, the late Queen of Tonga, is in an open carriage, waving and smiling to the spectators in the open street during Queen Elizabeth II's coronation in 1953 (see *Figure 8*). Koloto (2016) explains, the performance of the late Queen

emphasises the "*faa'i koula*" (four golden pillars) of Tongans: respect, humility, commitment and sense of responsibility (p. 2303).

The late Queen rode in an open carriage in the pouring rain to attend the coronation ceremony. Queen Salote showed *faka'apa'apa* (respect) (The Kingdom, 2018) through eagerness to uncover the carriage to be in the "shower of rain" (Gill, 2012) (p. 4) similar to all other outside spectators standing in the rain.

Figure 8: Late Queen Salote Tupou III

Source: (Printerrest, 2019)

Gill (2012), an attendee of the coronation day on 2 June 1953, stood beside the area where the arrival of an "elegant carriage", describes the Queen of Tonga as "a lady of compassion and matching girth, and a slightly built" (p. 4). Gill explains that there was an argument between the Queen of Tonga and a "diminutive man" (Portuguese Ambassador) who demanded to close the roof of the carriage. Queen Salote won the argument with the Portuguese Ambassador, and the carriage's roof remained open. After this, Mr Gill decided to visit Tonga. Gill took several visits to Tonga and the first visit was in 1970 (p. 4). An historic moment that attracted the

attention of audiences and media, and the action of the late Queen of Tonga "made her famous around the world" (The Kingdom, 2018) (paragraph 1).

2.5 Language

In this chapter, Tongan language is not only to explain the cultural features and communication benefits, but also that the language provides an opportunity to link to cybersecurity matters. Tongan words offer considerable chances to apply as strong passwords.

Mother tongue or native language symbolises identity and classifies the place, community, origin and culture. The mother tongue language is Tongan, and English is the second. The structure of Tongan words appears odd due to a mixture of alphabets, macrons and symbols. Here are examples of Tongan words to express the complexity of Tongan words: ʻēī, (hail), *māʻoniʻoni* (holy), *sōtia* (soldier), *fakalīfulifusia* (ilifia), *mālōlō* (rest), *Fālesi* (Pharisees), *Sāpate* (Sunday), ʻatā (space), *ʻalu ā ē* (goodbye) and more words.

The complexity of Tongan words enforces an additional security layer that is relevant to apply for strong passwords. Tongan words seldom appear in the English dictionary. A type of cyberattack is known for using words from the dictionary. Dictionary-attack works when a computer-user uses ordinary words or words from a dictionary as a password (Techtarget, 2021) which makes it easier for the cybercriminals to guess the password. As most of Tongan words are rarely exhibited in a dictionary, there is no chance for cybercriminals to deploy dictionary-attacks.

Laulaupea'alu and Keegan (2019) state that:

> People prefer to select easy-to-remember passwords which are considered to be weak and susceptible to another type of attacks such as dictionary-attacks. Strong passwords (combination of numbers, symbols, lowercase and uppercase alphabets, and a mixture of more than eight characters) is often hard to remember but the main advantage is difficult to guess by cybercriminals. A weak password offers more opportunities for the attackers to access the computer systems and a strong password is considerably harder for the computer systems to be compromised and controlled by attackers (p. 192).

Language-communication is in both Tongan and English. In primary and secondary schools, English is a compulsory subject where students must pass the English examination paper before moving to higher levels of education. Other educational institutes set rules for the students to speak English in school hours. Job interviews are conducted in English. The literacy rate, ability to read and write Tongan and English for ages 15 – 25 years, was "99" percent according to a report from Tonga Department of Statistics (2014) (p. xvii).

2.5.1 Division of Tongan words

Kaeppler (1971) specifies important characteristics of the Tongan language as the cultural hierarchical ranking or "societal ranking and the language of respect" (p.174).

Table 2 illustrates three divisions of Tongan words: the words for the commoners, nobles, and the words for the King.

Table 2: Division of Tongan words

English	**Commoners**	**Nobles**	**King**
eat	kai, mama	ʻilo	taumafa
run/walk	ʻalu/lele	meʼa	hāʼele
old	vaivai	mōtuʻa	toulekeleka
sleep	mohe	toka	tōtōfā
angry	ʻita	tuputāmaki	houhau
drinking kava	inukava	ʻilo kava	taumafa kava
dream	mohevale	misi	lika
yes	ʻio	ko/ ia	ko ē
mother	finemotuʻa	faʼē	fehuhu
see	sio	meʻa	ʻafio
work	ngāue	ʻuliʼi	maaʼimoa
teeth	maka	nifo	koloa
blood	toto	toto	taʻataʻa
sick	puke	tengetange	pūpūluhi

Division of words identifies societal rank where the commoners reside at the bottom of the hierarchical triad to uphold the cultural relationship and the respect to the

King at the top and nobles in the middle of the triad. '*Kai*' means eat for commoners, ''*ilo*' for the nobles and '*taumafa*' is uniquely exceptional to the King only. No one in the commoners or nobles is entitled to use '*taumafa*' or other words used for the King.

There are a lot of words, but these words mentioned in the abovementioned table are set to be examples of the hierarchical words for commoners, nobles and the King of Tonga. These words were taken from the local book publication named '*Ko e Talamalu 'o e Fonua'* authored by 'Ahio (2018) (p. 44 – p. 45).

2.5.2 Vowels and Consonants

'*Motu'aleá Faka-Tonga*' or Tongan alphabet consists of seventeen (17) words, twelve (12) consonants (*konisonaanite*) and five (5) vowels (*vaueli*) (Learn Tongan, 2017).

- 5 Vowels: **a** **e** **i** **o** **u** (5)
- 12 Consonants: **f** **h** **k** **l** **m** **n** **ng** **p** **s** **t** **v** **'** (12)
- To pronounce the consonants, a vowel 'a' is added to the end (Fa, Ha, Ka, La, Ma, Na, Nga, Pa, Sa, Ta, Va).

Fakau'a (glottal stop) is a consonant. It is the last letter in the *Motu'alea Faka-Tonga* and is not permitted to be placed at the end of a word. Also, the *fakau'a* is not allowed to be put between a vowel and a consonant (*a't, e'v, i't*), always placed in front of a vowel (*motu'alea, fakau'a*, '*ikai*).

- When the *fakau'a* is placed in front of a word, (e.g., '*ikai* means no), the first letter is the *fakau'a* (') but not the "i".
- Two consonants are not permitted to stand together in a word (ss, st, tf, kt, vt, ngt and so on).
- Consonants are not allowed to stand at the end of a word, which means that all words must end with a vowel(s).
- Vowels can stand and combine in two, three, four or more without any consonant.
- The ng is one consonant and represents only one sound or one pronunciation.

[FYI; *Appendix 2* (page 243) at the end of this thesis is a screenshot of a secondary school lecture note named '*Ko e Kalama 'o e Lea Faka-Tonga*', from where the above-mentioned information was taken. It is only one page from the lecture note that was photographed to confirm from where the original information came from].

2.5.3 Macron

Unilang (2019) specifies that Tongan language is an Austronesian group language and the oldest and most conservative Polynesian language. Austronesian language, formerly known as Malayo-Polynesian language, is spoken in the South and Central Pacific, New Guinea, Vietnam, Laos, Cambodia and Taiwan and is among the largest languages in the world according to (Britannica, 2020).

Unilang (2019) further expounds that the distribution and settlement of people in the Polynesian Islands originally came from Tonga and Samoa and then scattered to other Pacific Islands. Tongan language is very close and similar to other languages of Pacific nations such as Niue, Wallis Island (Uvea), Tuvaluan, Samoa, Tahitian, Hawaiian and Maori. In comparison with other Pacific nations, *motu'aleá Faka-Tonga* (Tongan alphabet) is the biggest (17 characters) in Polynesian. Hawaiian has thirteen and Samoa only fifteen letters (Unilang, 2019).

Table 3: Using of macron

Tongan words	**English meanings**	**Tongan words**	**English meanings**
mālōlō	rest	fānau	children
mālohi	strong	fāmili	family
pēpē	baby	mālō	thank you
fāngota	fish	'alu ā ē	goodbye
'univēsiti	university	la'ā	sun
Fēfē hake?	How are you?	mālō 'aupito	thanks a lot
'āua!	sure, exactly	mālō e 'ofa	thanks for your kindness
sai pē	just fine	mā'olunga	height
lōlōa	length	tānaki	gathering
fē?	where	Ke 'alu ki fē?	Where are you going?
hū	enter	ī	fan

The pronunciation of Tongan vowels is elongated by adding a faka‘ilonga toloi or macron (¯) over the vowels (ā, ē, ī, ō, ū). As soon as the macron is placed on top of the vowel, the pronunciation-speed of the vowel or word is doubled. Using double macron (¯) in a word, the stress and the pronunciation of the word falls on the last macron vowel. For example, in these words, fēfē or mālōlō or mālō, the stress falls on the last ‘e’ of the word fēfē and ‘o’ on mālōlō or mālō (Unilang, 2019).

Table 3 is a list of Tongan words and meanings with two or more macron (¯) signs are placed on the vowels. If the macron sign is not placed in a word, the meaning and the pronunciation of the word is different. For example, *pēpē* means baby. If the macrons are removed, no stress falls on the last ‘e’ and the word is pronounced *pepe* means butterfly. Like the word *mālōlō* (rest), if all macrons are removed from the word, no stress falls on the last vowel ‘o’ and the word *malolo* means bird. Notably, the macron (¯) is used for the vowel only but not for consonants (Unilang, 2019).

2.6 Population Distribution

In the 2011 census, Herbert (2013) produced a report about the annual increase of Tonga’s population. This is a 0.2 percent growth from 102,000 in 2006 to 103,000 in 2011. The number of households has increased by 3.4 percent from 17,462 in 2006 to 18,000. About 38 percent of the population is under the age of 15 and eight percent are 60 years and older. Also, “Tonga is predominantly rural – with only approximately 25 percent of people in urban areas” (p. 7). Based on the latest United Nations statistics (April 15, 2020), an updated data provided by World Meter (2020) shows the present population of Tonga is 105,440 with 24.3 percent (25,648 people) residing in the urban area. Also, Tonga’s total land area is 720 km^2 (278 square miles) and the population density is 147 per km^2 (380 people per mi^2) (World Meter, 2020) (paragraph 1).

Herbert (2013) also provides figures of how the Tongan population is distributed to each region (see *Table 4*). Tongatapu, the largest island, is occupied by almost 73 percent and the remaining 27 percent is scattered throughout the other four regions.

Table 4: Population distribution of Tonga

Region	Total population	Percentage of Population (%)
Tongatapu	75,158	72.95
Vava‘u	14,936	14.50
Ha‘apai	6,650	6.45
‘Eua	5,011	4.86
Ongo Niua	1,281	1.24
Total	**103,036**	100

Source: (Herbert, 2013)

FAO (2011) informs that poverty is one of the major push factors for internal migrations from rural to urban areas. This statement is real in Tonga as internal migrants have shifted from remote islands to get access to better services and economic welfare. Regardless of congestion issues and urban challenges, majorities are keen to take advantage of urban beneficiaries. Upon settlement in Tongatapu, the most convenient point to link overseas, internal migrants then look for “attractive destinations overseas” (p. 5) to find a better life.

2.7 Location and Isolation

Tonga, a small island located between Australia and South America, is in the middle of the South Pacific’s Ocean. The Pacific Ocean is the deepest basin and largest ocean in the world, reaching an average depth of 4,000 metres (13,000 ft) and scattering around 155 million km^2 (60 million m^2) (Oceania Exploration, 2021). The Kingdom of Tonga is ranked in 194^{th} position of land area in the world with a 30 km^2 of water and 717 km^2 of land (i.e., a total area of 747 km^2) (World Atlas, 2021). The location of Tonga is positioned at 173^0 west longitude 22^0 south latitude above the Tropic of Capricorn and south of the equator (FAO, 2011).

The International Date Line (IDL) is an imaginary line to separate two consecutive calendar-dates that crosses through the centre of the Pacific. *Figure 9* displays an image of the Pacific islands and the IDL (red dotted line), located on the 180^0 longitude, which separates the eastern and western hemisphere (World Atlas, 2019).

Figure 9: International Date Line

Source: (Lewis, 2015)

The IDL is vertically drawn from the North Pole down to the South Pole. As the IDL touches the equator, it bends to the right through Kiribati, Samoa and Tonga. Regions falling to the west of IDL have the same date such as New Zealand, Kermadec, Chatham, Tuvalu, Tonga, Fiji, Wallis and Futuna, Tokelau and Samoa. Whereas regions that fall at the east of IDL such as French Polynesia, Niue, Cooks Islands, American Samoa and Hawaii are lagged one day (Lewis, 2015).

2.7.1 Internal Isolation

Outlying Ongo Niua islands (Niua Fo‘ou and Niuatoputapu) to the northern province (shown in the Map of Tonga in *Figure 7*) separates these two islands from the rest of Tonga. Irregular goods delivery to this region is a consistent issue, as delivery depends on inter-ferry timetables and weather conditions. Wharves for bigger ships to berth are major issues for these two islands to load/unload cargoes.

Figure 10: MV 'Otuanga'ofa at Niuatoputapu

Source: (Loop Tonga, 2018)

Figure 10 identifies major issues facing Ongo Niua. MV ‘Otuanga‘ofa is unable to land at the wharf as the sea is very rough. The passengers and goods are loaded to a small boat and transferred to/from to the land/ship respectively.

Transportation, domestic airways and interisland ferry are the major issue for regular goods delivery and government services. An important event in Tonga, the survey of household income and expenditure, was conducted by Tonga’s Statistics Department in 2009. The actual plan for this survey was approved to be conducted in four phases. Implementation of the survey was carried out successfully in other main regions of Tonga except for the Ongo Niua where the interview and data collection were taken place at once. According to the Statistics Department (2010), the exception was related to the Tsunami that happened in September 2009 and the transportation issues, irregularities of both domestic flights and inter-ferry shipment.

Ha‘apai Group, a total of 51 islands, is scattered across a total area approximately 13,000 km^2 (5,000 square miles (Britannica, 2019). Interisland transportation is a major challenge due to bad weather and the high cost of petrol. Rising petrol costs is one of the main problems as the main interisland transportation is normally open-

wood boats powered by an outboard motor. Gasoline prices in Tonga have reached to over Top$3 per litre. Today's price (May 23, 2019) is TOP$2.82 per litre according to (Numbeo, 2019)

The main issue of goods delivery faced by Ongo Niua is the remote islands of Ha'apai. There are fixed destinations assigned for the main interisland ferry to be anchored. Locals travel from their isolated islands in open boats to load/unload the passengers/goods to/from the main ferry and then return respectively. The upload/unload process is carried out on the open sea, without wharf, mainly in the nighttime as the ferry program is timetabled to anchor in Pangai, the capital of Ha'apai, early in the morning. Despite the rough, open sea and expensive petrol, locals must come to the main ferry to collect their goods or passengers.

2.8 Economics

In Tonga, local citizens rely on subsistence farming and local fishing to earn a living. Citizens cultivate their own subsistence work, growing and gathering local food or fishing, to feed the families. According to a report from the Statistics Department (2014), the total number of fixed paid workers aged 15 years and above was 23,698 individuals. About 9,549 workers are in the subsistence work category that is 40 percent depend on their work to earn living.

Generally, Tonga is not in a critical position to classify in the poverty category. Herbert (2013) expounds that "poverty is rare in Tonga" (p. 2). Despite the rarity in poverty, locals migrated overseas because of "limited natural resources" (Otsuka, 2007) (p. 452) and less "opportunities for socio-economic advancement" (FAO, 2011) (p. 7). Otsuka (2007) also confirms that job opportunities are limited as the unemployment rate for ages 15-24 years was "11.9 percent" (p. 452) as according to a survey conducted by Tonga Statistics Department in 2005.

2.8.1 Migration

Internal migration within the regions is a regular procedure in Tonga as there are no regulations to hinder the free internal shifting of locals from one region to another region. The internal migration reflects demands for economic and infrastructural advantages of urban modernisations. Ketu'u (2014) confirms an increase of 0.5 percent in the urban area after the 2011 census. The majority of the migrants came from the remote four islands (Vava'u, Ha'apai, 'Eua and Ongo Niua)

to Tongatapu. Ketu'u also stated that "the population movement reflects the greater opportunities and better infrastructure that is available on Tongatapu and, in particular, Nuku'alofa" (p. 62). FAO (2011) confirms an additional number of 9,342 migrants to come to Tongatapu were "mainly from Ha'apai" (p. 10).

An example of the need for better health facilities in Tongatapu is proved by the childbirth rate in 'Eua (only two hours by ferry or seven minutes by plane). Only 61 percent of the babies were born in 'Eua in 2006. The Eua mothers took temporary migration from 'Eua to Nuku'alofa to give birth in "Tongatapu where maternal facilities are better at the main hospital" (FAO, 2011) (p.10).

An economical issue has been discovered by the increase in household expenses. This is due to the unstable shifting of agricultural labourers from one place to another with no time to grow food for families. Temporary migration under the Recognised Seasonal Employer (RSE) scheme has also reduced the local agricultural food supply as RSE labourers spend months working overseas. Local families rely on remittances from RSE workers to purchase food.

FAO (2011) conclude that RSE migrants:

> ……. work overseas for seven months of the year leave only five months at home to continue subsistence farm operations. This five-months period is too short for the crop cycle of any of the main food crops in Tonga, in particular the longer term root crops. The five-months home break does not allow much time for farming activities as other home chores such as house maintenance and building may also need doing, and take priority, leaving little time for planting crops (p. 9 - 13).

Ravulo (2015) reports that the total number of Tongans residing in Australia is 25,096 and most of the Pacific people live along the east coast of Australia. The largest number of migrants were Maori, Samoa in second, Tonga in third, and Fiji in fourth place.

FAO (2011) summaries a report from CIA World Factbook in 2010 that 55 percent of Tongan migrants resided in Australia and New Zealand. "36 percent were in North America, five percent in Asia, two percent in Europe" (p. 8) and one percent in other nations such as Caribbean, Africa and Latin America. In Australia, religious

missionaries offered Tongan students to train to be nurses, pastors and teachers in Victoria in the 1930s and 1940s. In 1947, the Victorian census recorded 31 new Tonga-born Victorians. “This number increased to 80 by 1971, 300 by 1981, and 800 by 1991 and by 2006 there were 1190 Victorians who had been born in Tonga” (FAO, 2011) (p. 7).

An important philosophy was brought in by Nicky Gumbel, the developer of Alpha Course in the UK, about the power of the city in terms of culture. City, in a certain characteristic, a place where culture is developed or formed. “The river of influence tends to flow from the city to the suburbs and rural areas. The way to transform a culture is to transform the city” (Gumbel, 2020) (paragraph 3).

Based on the information above, migration in Tonga is a process of moving from one area to live in another area to find more opportunities. Opportunities include education, a better place to live, employment, healthcare facilities and other urban benefits. Migration’s major push-factors, typically negative things, are generally related to unemployment, droughts, crop failure, war, poor services, flooding, poor education and so on. On the other hand, pull-factors, usually positive things, attract the attention of migrants to leave their home nation because of a better standard of living, better education, job opportunities, or better healthcare (Tekstas, n.d.). Comparatively, other nations migrate overseas due to conflicts, fights, clashes, overcrowding, drought and war. In Tonga, no issues are regarded to these push-factors especially drought and civil wars. Today, climate change, a major worldwide concern, is a major push-factor for low coral islands in the Pacific to migrate to other high topography and wealthier nations.

2.8.2 Overseas Remittance

Herbert (2013) reports that the number of Tongans in the US, Australia and New Zealand is estimated to be around 150,000, which is approximately 1.5 times the size of the population in Tonga. Migrants remit money home – “a total of 21 percent of total income of Tongan households in 2009” (p. 9). Another report from FAO (2011) states that “Tonga is the world’s second highest recipient of remittance flows relative to the size of its economy which contributed 39 percent of Gross Domestic Product (GDP) in 2007’ (p. 5).

Ketu'u (2014) conducted a survey to clarify more information about overseas remittance. Here is the summarised information that Ketu'u collected from the survey participants in Tonga:

- Survey participants with children overseas were remitted money on a very regular basis (p. 166);
- Some of the old participants mentioned that remittance was their only source of income (p. 166);
- One old participant mentioned a monthly average of TOP $500 pa'anga is regularly remitted from three children overseas (p. 166);
- Apart from the regular monthly remittance, the same old participant mentioned that extra money was also sent for *ngaahi pola konifelenisi* (conference feast) in May and misinale (annual church donation) in November every year (p. 166).

Tonga Development Bank (2016) 'Ave Pa'anga Pau is a programme to assist Tongans overseas to transfer money (online) to Tonga using portable computer devices. A price giving programme organised by TDB in early 2020 aims to encourage overseas Tongans to remit funds home through the 'Ave Pa'anga Pau programme. The prize was won by one of the New Zealand RSE workers. *Figure 11* shows the winner of this competition, John Tali and TDB staff, after the prize-giving ceremony (Facebook, 2020).

RSE is a seasonal programme that allows Pacific islands' able workers to work on farms in New Zealand and Australia. According to the Acting CEO of Tonga's Internal Affairs, the RSE programme raises Tonga's economy in different ways. RSE New Zealand was first introduced in 2007 with more than 14,000 Tongan employees to collect NZD$81 million from 2007 to 2018.

RSE Australia employed more than 10,000 Tongan locals since the programme started in 2012 with about AUS$99 million injected to Tonga's economy (Tonga Broadcasting Commission, 2018b). Updated news about Tongan RSE workers during COVID-19 health crisis, the Australian government has extended their working visas for 12 months due to shortage of farm labourers. Workers are exempt from lockdown rules based on an essential services basis, and employers are responsible to keep employees out of virus infection. This extension provides great opportunities to assist families in Tonga (Kaniva Tonga, 2020).

Figure 11: 'Ave Pa'anga Pau Winner John Vala (left)

Source: (Facebook, 2020)

Like New Zealand RSE, employees in the essential work category can work during the Alert-Level 4 lockdown. Essential work includes picking, packing, packaging, viticulture and horticultural production for overseas and local markets. RSE employees are eligible for government entitlement if they fall sick. If a company is affected and closed due to the Alert-Level 4, employers are entitled to apply for a government wage subsidy to pay the employees. At any stage where the Ministry of Health recommends ceasing work due to health issues, RSE workers are also eligible to apply for Essential Workers Leave Support which equates to NZ$585.50 per worker/per week. Due to the limited face-to-face services, RSE workers are

encouraged to send money back home by using online banking services (Devpolicy, 2020).

2.8.3 Economic comparison between Tonga and Samoa

Gross Domestic Product (GDP)

A quick revision of figures and numbers to compare the national income and output or the total expenditures for all goods and services produced in Tonga and Samoa. GDP is not only the monetary value of a nation but also an indicator to measure the health of a nation's economy within a specific period.

Table 5: Tonga GDP vs Samoa GDP

Tonga GDP					
Period	**Actual**	**Previous**	**Highest**	**Lowest**	**Unit**
1975-2019	0.46	0.45	0.47	0.03	USD Billion
Samoa GDP					
Period	**Actual**	**Previous**	**Highest**	**Lowest**	**Unit**
1982-2019	0.90	0.86	0.90	0.10	USD Billion

Tonga's GDP was USD$ 0.46 billion in 2019 which only contributed less than 0.01 percent of the total economy of the world (Trading Economics, 2019c). Samoa's GDP was USD$ 0.86 billion in 2018 which only contributed less than 0.01 percent of the total economy of the world GDP (Trading Economics, 2019a). Samoa's GDP was USD$0.90 billion from 1982 – 2019 while Tonga's was USD$0.46 billion from 1975 – 2019. Samoa's GDP is 51 percent stronger than Tonga's GDP as at the end of 2019 (see Table *5*). These figures were taken in April 2020 and are subjected to change periodically.

GDP per Capita

GDP per capita measures the economic stability and the way the GDP is divided among the total population. (a country's economic output divided by total population). The figures in *Table 6* are GDP per Capita of Tonga and Samoa and were taken in April 2020. These figures are subjected to change periodically.

Tonga's actual GDP per Capita was USD$ 5,696.20 in 2018 and it was reached to USD$5,746.00 in 2017 (Trading Economics, 2019d). Samoa's actual GDP per

Capita was USD$6,089.30 which was the highest amount reached in 2018 (Trading Economics, 2019b). Samoa GDP per Capita (USD $6,089.30) is stronger than Tonga GDP per Capita (USD $5,696.20) with a difference of only USD $393.10 GDP per Capita.

Table 6: Tonga GDP per Capita vs Samoa GDP per Capita

Tonga GDP per Capita					
Period	**Actual**	**Previous**	**Highest**	**Lowest**	**Unit**
1990-2018	5696.20	5746.00	5746.00	3577.40	USD
Samoa GDP per Capita					
Period	Actual	Previous	Highest	Lowest	Unit
1990-2018	6089.30	6069.30	6089.30	3485.10	USD

Herbert (2013) conducted a review of political economy, analysed social economy and examined poverty in Tonga in 2013. Some of the report findings discovered that:

- A total of TOP$355,856,000 pa‘anga (Tongan households’ income) in 2009; 43 percent from wages and salary; 29 percent of income from subsistence + home produce activities; and 21 percent from remittances.
- A total of TOP$333,027,000 pa‘anga (Tongan households’ consumption expenditure) in 2009, 51 percent for food expenditure, 11 percent for transportation and 10 percent for housing and utilities (p. 2).
- Tonga is ranked in the Upper-Middle-Income-Country (UMIC) category “without absolute poverty”.
- Human Development Index ranked Tonga to be 85 out of 169 nations in the UMIC and “one of the highest in the Pacific Islands” to reach the UMIC position.

UMIC is classified for the nations with the GNI (Gross National Income) per capita between $4,046 and $12,375 (The World Bank, 2020) (paragraph 1). Although Tonga is under the UMIC category, the Kingdom nation is listed by the United Nations (2014) to be under “small island developing states” (p. 150). ENotes (2019) states that developing countries are still experienced with many issues which, in fact, that they (developing countries) are poor. Life expectancy is low, as is the low

affordability of good medical resources and poor education as people cannot afford to meet education needs and pay good teachers. Also, ENotes (2019) mentions that competition in the global economy is difficult due to low-skill workforce and poor educational knowledge. Lack of good education hinders the growth of development. Poor governance is also a major issue as the Government is unable to pay well-paid officials for management.

2.9 ICT Connectivity

World Bank Group (2020) raises one of the challenges to ICT connectivity in Tonga. This is due to the geographical isolation of 76 inhabitant islands across 700,000 km^2 of ocean. The International Development Association (IDA) had donated US$16.03 million to Tonga's Pacific Regional Connectivity Programme (PRCP). Another US$0.46 million was contributed to Tonga PRCP by Australia and New Zealand's Pacific Regional Infrastructure Facility (PRIF) Trust Fund. These donations aim to facilitate and deliver reliable, advanced and more affordable ICT services.

ICT connectivity in Tonga is materialised by modern light-transmission-data fibre-optic cable. An 826 km undersea cable connection is stretched between Fiji and the main island Tongatapu, funded by a grant from World Bank, Asian Development Bank, and Tonga Corporation in 2013. After this major ICT transfiguration, the internet speed "was shifted 20–30 megabytes per second to 10 gigabytes per second" (S. Laulaupea'alu & T. T. Keegan, 2018) (p. 255).

Interisland distribution of the fibre-optic cable from the main cable centre in Nukuʻalofa, (see *Figure 12*) has been outreached to the other two main regions of Vavaʻu and Haʻapai. Redline on the map denotes the undersea pathway of the domestic fibre-optic cable. The outreach of this 400 km cable is the second phase of the original underwater Southern Cross Fibre-Optic Cable Network (SCFOCN) connection from Fiji. The domestic extension to reach Vavaʻu and Haʻapai was completed in April 2018 (Tonga Broadcasting Commission, 2018a).

TCC, fully owned by GoT's Internet Service Provider (ISP), launched a new UCall mobile service to Niuafoʻou Island, commissioned by His Majesty King Tupou 6 on 7th August 2014 (Matangi Tonga, 2014). The new UCall service is added to the fixed-line services already installed on this remote island. Other remote islands

already involved in the UCall service were Nomuka, Ha‘afeva and Niuatoputapu. According to TCC officials, despite the high cost of providing this service, the mission of the TCC is to outreach so people can share the benefits of communication technology.

Figure 12: Domestic fibre-optic cable

Source: (Moala, n.d.)

An ICT proposal is under negotiation between the GoT and Kacfic Broadband Satellites Group. A 15-year agreement between the GoT and Kacific to outreach connectivity to 89 remote islands through high-speed satellite. This proposal was negotiated after the fibre-optic cable outages that disrupted the whole nation’s ICT connectivity in January 2019. A physical breakdown of the submarine fibre-optic cable turned down the internet connection for 12 days. This proposal provides an opportunity for a backup to standby for future malfunctions of the fibre-optic cable. Also, the connectivity plan is to outreach the ICT network to cover the remaining rural and remote areas. Remote islands can access to e-government services such as police, hospital, post office, education, clinics and dispensaries (ZDNet, 2019).

Papacharissi and Zaks (2006) state that the maximum high speed advertised by ISP is approximately 400 kilobits per seconds (Kbps). As previously mentioned by

Laulaupea‘alu and Keegan (2018), the internet speed of Tonga was “10 gigabytes per second” (p. 255) in 2013. An early report from ITIF (2019) confirms the fibre-optic cable transmits “over 200 terabits per second” (p. 1).

A simple calculation of the internet speed in Tonga is to be taken based on the speed of 400 Kbps mentioned by Papacharissi and Zaks (2006) versus the speed of 10 gigabytes per second provided by Laulaupea‘alu and Keegan (2018).

A simple calculator tool is taken from GbMb (2019) to carry the calculation to identify the existing fibre-optic cable and proposed satellite speed .

- 1 gigabyte = $8x10^6$ kilobits
- 10 gigabytes (the internet speed of Tonga in 2013) = $8x10^7$ kilobits per second
- 400 Kbps = $8x10^7$ x 400 = $32x10^9$ Kbps
- Therefore, the proposed speed is $32x10^9$ Kbps slower compared to the speed of $8x10^7$ Kbps in 2013.

Chron (2019) clarifies some weaknesses of the satellite connection. The satellite internet connection uses Microwave Radio Frequency (MRF) which transmits in a straight line. MRF is unable to pass through a solid object. Bad weather and moisture hinder the signal between the satellite and the dish. At some stage during a thunderstorm, heavy rain can interrupt and completely block the signal. Even in good weather, ice and snow can build up on the dish and block the signal. Severe storms, hurricanes and tornadoes can rip the dish. Obstruction of a solid object, such as a tree, wall, house or tower, can also block the MRF signal. There is no snow in Tonga to block the MRI transmission.

Hurricanes, cyclones, tornadoes, and storms are the major natural disasters affecting ICT connectivity. The hurricane period ranges for many months during the warm season. Hurricane season destructs from November to April every year. Tonga was destroyed by a heavy cyclone, Gita, in February 2018. A historical category 4 cyclone caused major destruction to the main island of Tongatapu (see *Figure 13*)

Figure 13: Cyclone Gita visited Tongatapu in 2018

Source: (BBC News, 2018).

The new satellite proposal will play momentous gains to serve the remote islands and rural areas and will stand by for future accidental damage to the existing fibre-optic cable. New satellite proposal must ensure that the exposure of disks and telecommunication physical components will withstand the regular visit of cyclones to Tonga.

2.10 Tongan Culture

Koloto (2016) states that the combination of Tongan culture (four core values or four golden values) "bind together the Tongan culture" (‘*ulungaanga-fakaTonga*) These four core values, known as "*faai'i kavei koula*", are *faka'apa'apa* (respect), *lototō* (humility and generosity), *tauhi-va* (loyalty and commitment) and *mamahi'ime'a* (sense of responsibility and commitment to the cause) (p. 2303). Fehoko (2016) adds another value of ‘*ofa* (p. 12) to the Tongan culture. Baker (1897) defines ‘*ofa* is "Love, affection, esteem: a fathom, or the measure of the arms extended" (p. 15). Further, Fehoko (2016) (p. 61) and Koloto (2016) (p. 2304) are both agreed that the *faai'i kavei koula* (four golden values) of Tongans plus the inclusion of ‘*ofa* (love) are attributed to the well-known story of Late Queen Salote Tupou III of Tonga and the coronation of the UK Queen Elizabeth in 1953. (Summary of the coronation event-story is explained in this thesis in the Coronation Section 2.4.1).

Fairbairn-Dunlop (2015) expounds the importance of "'*ofa* (love)" as it drives all the Tongan cultural values (four golden values) together (p. 14). Tafea (1999) adds '*ofa* (love) to the existing four values and concludes that these Tongan values (five core values) assist in preserving the monarchical system in Tonga. Bennardo (2008) summarises comments from one of the Tongan scholars, Sione Langi Kavaliku, to explain *'ofa* as the treasure of Tonga and the philosophy behind their way of life. More meanings related to '*ofa* are care, concern, gift, help, hope, kindness, sadness, sexual love, and sharing. Kavaliku concludes that the usages of 'ofa show the kind of relationships between members using the term and that we could not comprehend or understand *faka'apa'apa* (respect) unless we understand 'ofa".

2.10.1 Faka'apa'apa

Vaioleti (2006) defines *faka'apa'apa* as respect, consideration and humility. Taumoefolau (2013) states that "respect (in Tonga) is expressed in the way of behaving and way of speaking" (p. 119). For example, wearing a *ta'ovala* (waist-mat) is an indication of expressing respect like westerners wearing a suit and a tie.

Vaka'uta (2009) expounds *ta'ovala* is not simply dressed as a symbol of respect, but to specify variances "in social status, and differences between occasions" (p. 132). Different *ta'ovalas* are worn in time of celebration and in time of mourning. Black, ragged mat *ta'ovala* or *ta'ovala-motumotu* and dark brown signify funeral. A *ta'ovala-lokeha* (waist mat-made from pandanus tree) and *ta'ovala-fau* (waist-mat made from *fau* tree) are normally worn by the Government employees as Tongan traditional suit or worn to churches or meetings or feasts or celebrations.

In funeral, the people who are known as *liongi* (lowly role at the funeral) wear "ragged mats" (James, 2002) (p. 225) or *ta'ovala-motumotu* which identify the position as a *tu'a* (commoner) (Vaka'uta, 2009) (p. 128) (commoner or ordinary non-chiefly people) (Taumoefolau 2013) (p. 120) to the deceased. The *liongi*-women hang down "their hair loose in an unkempt way" (p. 225) to show respect. The roles of the *liongi* are to *nofo he afi* (stay beside the fire) to cook and to serve the food for the mourners during the whole night of the *'a-pō* (last night farewell with the deceased).

Figure 14: Hon Tuita's family wearing ta'ovala

Source: (Wikipedia, 2021).

Princess Pilolevu Tuita (see *Figure 14*) with family members appeared during the grief of the Princess's father, the late King Taufa'ahau IV who passed away in 2006 (Wikipedia, 2021). Princess Pilolevu Tuita, the only daughter of the late King, accompanied with other immediate family-members, displays respect by dressing in black cloth with hair loose and wearing *ta'ovala-motumotu* (ragged mats). The process of wearing *teunga-'uli* (black cloth) and *ta'ovala putu* (funeral waist-mat) is known as *tauanga'a* (worn black). Children of deceased victims are voluntarily worn *tauanga'a* for one whole year. In Tonga, no rules for *tauanga'a* but immediate family-members are willing to show *faka'apa'apa*, *tauhi-vā*, *mamahi'ime'a, lototō,* and *'ofa,* to the deceased.

The expression of *faka'apa'apa* within the nuclear family is unique. A traditional *tabu* or *taboo* (forbidden) is set to separate brother and sister. A brother (*tuonga'ane*) and sister (*tuofefine*) are not allowed to sleep in one *fale* (Tongan house). Respect or "*faka'apa'apa 'a e tuonga'ane ki he tuofefinee. 'Ikai tena mohe ha fale 'e taha*" (Vaioleti, 2006) (p. 28). In English translation, the respect of brother to sister is not allowed to sleep in one house.

Argument, battle, swearing or hateful words between sister and brother are prohibited. Any stage where traditional taboo is unfollowed (battle, enter sister room and so on), brother and sister are known as *'ikai akonaki'i* (not giving the

right advice). *'Ikai akonaki'i* is claimed to be the parents' irresponsibility for not giving the right advice to the children. *'Ikai akonaki'i* then ends up in *fakamā* (feeling embarrassed, uncomfortable or ashamed) and affects the parents' reputation and counts as a long-standing rumour for the family.

M*ehikitanga* (father's sister) is the *fahu* and takes the "highest rank and most 'eiki (privileged) position in the extended family" (Koloto, 2016) (p. 2305). *Fahu* means "above the law" (James, 1983) (p. 236) (Kaeppler, 1971) (p. 177 & 178) (Biersack, 1982) (p. 188). The father's children call their father's sister as *mehikitanga* (aunty) or *fahu*.

Kaeppler (1971) expounds the power of the *fahu* and the meaning of the phrase 'above the law'. "A *fahu* may go to the farm and take a pig without even asking" (p. 177) the owner (brother). In funerals, the *fahu* sits in front of the deceased person during the last night farewell with the deceased ('*a-pō*). Funeral attendees and families come with gifts of fine mats, tapa clothes, food and money to give away to the *fahu*.

Tonga relies on subsistence farming as one of the main sources of food. Rennie (1991) confirms that "women did little in agricultural work (and the women who are the *fahu*) could rely on their brothers or maternal uncles" (p. 9). Conclusively, females, especially *tuofefine* (sister) and *mehikitanga*, (aunty) are very special and considered to be above the law or *fahu* in Tongan ways of living.

Polopolo

Polopolo is an act of giving the first and finest yield (Prescott & Hooper, 2009) to special individuals. *Polopolo* is an offer or giveaway of the farm produce from *ma'ala* (yam plantation) or any sort of crops on the first harvest day. *Polopolo* allows permission to start the harvest, and the first step is to give away the *fuatapu* or '*uluaki-fua* (best yields) to locals. Without giveaway of the *fuatapu* or '*uluaki-fua* then this process is not worth to calling *polopolo*. As customary, the growers pick up the best produce (like yams, taro, *kumala* and other crops) and offer to the chief (*hou'eiki*) of the village, widows, *mehikitanga* (father's sister), *tuofefine* (sister), and the owner of the land.

Francis (2009) describes *toutu'u* is a "collective garden" (p. 207). This is a traditional way of gathering locals to form a group to plant similar types of crops in

a piece of land offered or belonging to a person. In the time of *polopolo*, all the *toutu'u* members choose the *fuatapu* or '*uluaki-fua* (best yields) as '*inasi* ready to offer, deliver and give away to respective locals. Aswani and Graves (1998) define '*inasi* as "a share or portion of anything that is to be, or has been, distributed out" (p. 145).

Figure 15: Giving of 'inasi to the King

Source: (Picclick, 2021)

Figure 15 is a picture of the first fruit ('*inasi*) ceremony (Picclick, 2021). The image was drawn by John Webber, (Captain Cook official artist) at the village of Mu'a, (the old capital of Tongatapu) during the voyage of Captain James Cook to Tonga on 10 June to 10 July 1777. Pictured at the centre of the image is the son of the King of Tonga surrounded by the *matapules* (talking chief) and the paired carriers with symbolic '*inasi* knotted to a horizontal *ha'amo* (pole/stick) (Classical Images, 2019). James (2002) describes *matapule* as a man chosen to be a "representative, spokesman, or herald" (p. 225). The King of Tonga and the nobles choose, give authorities, titles, and names to the *matapule* and act as representatives respectively.

The giving of the '*inasi* to the King is an "important national ceremony" (Latukefu, 1975) (p. 2). In preparation to give the *'inasi*, the *hou'eiki* (chief/noble) gathers together the *matapule(s)* (chief attend(s)) and the people of the village to be ready

to visit the King. All the attendees must wear the Tongan traditional costumes and gather in one group ready to present the '*inasi* to the King's *matapule(s)*. The *'inasi* is the best of all kinds of food groups, seafood, handicrafts and other traditional items to be taken to the King.

Father's taboo

According to Latukefu (1975) (p. 7), children are forbidden (*tapu* or taboo) to: touch the father's hair or head; to eat or share the father's remaining food; standing near or eat while sitting on father's lap; to touch the father's personal belongings.

Taboo is not particularly targeted to nuclear families but is further extended to include extended families such as brothers, cousins and *mehikitanga* (father's sisters). The important point in the *taboo* or *tapu* is the speciality of the *mehikitanga*. Douaire-Marsaudon (1996) highlights the features of *tapu* and the respect of father's children to the *mehikitanga* (father's sister):

> A child must respect his father and his father's brother who are in many ways tapu to him; but to his father's sister (*mehekitanga*), he must pay even greater respect. It is she who is really supreme in the family. Her person, food, clothes and bed are tapu; she often controls the matrimonial destinies of her brother's children (p. 139).

With the rejection of the *tabu*, a *mala* (misfortune for wrongdoing or penalty) which leads to *mala'ia* (bad luck) of breaking the *tapu*. The early death of children is believed to be "the failure to observe these taboos" (Latukefu, 1975) (p. 7).

2.10.2 Tauhi-vā

Tauhi is to "take care of, tend to, to look after", or a "person who takes care of another person, items or place" (Koloto, 2016) (p. 2303). '*Vā*', similar to the Maori word 'wā', is referred to the distance or "space between social relations, socio-spatial relations, or space that relates" (p. 2303). To combine these two words into *tauhi-vā* means "to look after or protect the *vā* or space between two or more people or among groups who are related to one another in some way" (Koloto, 2016) (p. 2303). Also, Pau'uvale (2012) defines *tauhi-vā* is the act of "maintaining positive relationships with one another" (p. 84 – 85).

Tauhi-vā covers multiple ranges within *nofo ʻa kainga* (extended family's ways of living). *Tauhi-vā* within *nofo ʻa kainga* is the *tauhi-vā* or to maintain the relationship between father vs mother, relationship between parent vs children, relationship between brother vs sister, relationship between brother vs brother, relationship between grandparents vs children, relationship between the father's sister vs children, relationship between uncle (*faʻee-tangata* or mother's brother) vs children, and more *tauhi-vā* within *nofo ʻa kāinga* (Koloto, 2016)

Koloto (2016) further extends the process of *tauhi-vā* to include:

- *Tauhi-vā* mo e ʻOtua (Nurturing relationship with God)
- *Tauhi-vā* mo e Tuʻi ʻo Tonga (Nurturing relationship with the King)
- *Tauhi-vā* mo e Houʻeiki (Nurturing relationship with the nobles)
- *Tauhi-vā* mo e Siasi (Nurturing relationship with the church)
- *Tauhi-vā* mo e Fonua (Nurturing relationship with the land) (p. 2304).

Koloto (2016) clarifies that whenever the *vā* is misbehaved, then the *vā* is *kovi* (bad) or *vā-tamaki* (bitter) causing the barrier in the interflow of interaction that leads to a sad or bad relationship (*vā kovi*). "Such *vā kovi* may eventually lead to the motu or motuhi (break-up) of the vā. To maintain a *vā* ʻ*oku moʻui* (live and healthy *vā*) and *vā* ʻ*oku lelei* (harmonious and good relationship) is the ultimate purpose of *tauhi- vā* (p. 2304).

Koloto (2016) concludes "the *tauhi-vā* by people in the past may benefit those in the present and the *tauhi-vā* by people in the present will benefit those in the future" (p. 2306). Tevita (2005) points out the remittance of funds from overseas-Tongans to families in Tonga is a "transnational *tauhi- vā*" (p. 101-102). Herbert (2013) states that around 150,000 people of Tonga live in the United States, Australia and New Zealand (approximately 1.5 times Tonga's population) contributing 21 percent to Tonga in 2019. Overseas remittance is not only to raise the local economy but also a sign of *tauhi-vā* and *ʻofa* (love) or *ʻofa fonua* (love the nation).

2.10.3 Mamahiʻimeʻa

Kalavite (2010) translates the Tongan word *mamahiʻimeʻa* as "loyalty and commitment" (p. 41). To be loyal and committed means to keep the *fatongia* (role, obligation, and responsibility) to the *fāmili* (family), *siasi* (church) and *fonua* (land and people). In the process of *mamahiʻimeʻa*, Tongans must successfully fulfil the

utmost obligations to the communities (*fāmili*, *siasi* and *fonua*) as well as education. Pau'uvale (2012) refers *mamahi'ime'a* as "social obligations or *Ngaue Fakataha fika 'uluaki*" (p. 84) or the prioritising of working together or team spirit (p. 15).

Further, Kalavite (2010) sets an example of *mamahi'ime'a* in one of the schools owned by the GoT. Tonga College, A secondary male-boarding school with the motto is known as *Mate ma'a Tonga* (Diehard for Tonga). Students are encouraged to practise the school's motto in all places within school and outside school. All the golden values (*tauhi-vā*, *mamahi'ime'a, 'ofa, lototō,* and *faka'apa'apa*) are practised and inherited in the school for many decades. The *kau-matāpule* (college prefects) take the roles and responsibilities of parents and teachers to discipline the students. The voice of *kau-matapule* is very loud and is respected by the students. In respect and inheritance, students always *talangofua* (obey) and follow the words and announcements provided by the *kau-matāpule*.

In the first week of the *fokotu'u 'a e ako* (beginning of school), a special programme for the new students called *fakalatalata* (an act of trying to be interested in a new place). The act of *fakalatalata* includes the enhancement and preparation of new students to be a *tangata-kakato* (full-man), *tangata-lahi* (big man), *tangata Kolisi Tonga mo'oni* (true Tonga College man) and to remember the school motto *"Mate ma'a Tonga* (Diehard for Tonga).

A long-standing cultural practice highlights the respect of the students to the *kau-matāpule*, teachers and staff. This practice is inherited and passed from the matured students to the new generation (students) to keep this culture alive. For example, if a *matāpule* or a teacher walks on the footpath, students who are close, walking close, or coming in front, must step aside to clear the pathway to allow the *matapule* or teacher or the staff to walk past. This cultural practice has been inherited for many decades and is unique in Tonga College.

[FYI: There is no academic reference for the above information. However, the author of this thesis was a *matāpule* (prefect) in Tonga College and these cultural practices were inherited from generation to generation]

2.10.4 Lototō

Kalavite (2010) defines *lototō* as generosity, modesty, humility or being subservient (p. 36 - 40). Richards (1988) defines humble as "a low estimate of oneself" which

is a "man who accepts his lowly position as what is due him is the man who has humility, or the humble man" (p. 253).

Cambridge Dictionary (2020) defines the meanings of subservient, generosity and modesty are as follows:

- subservient: to consider, wish or aim to be less important than the other
- modesty: not talking about or not prevent showing off to other people about abilities and achievement
- generosity: willing to give support or help, especially more than is expected and usual

Additionally, Kalavite (2010) defines *lototō* as the eagerness, willingness or "mental readiness" of Tongans "to do something". Tongans are not humble, boasting, self-praising or willing to show off the capabilities and achievements in "front of other people". *Lototō* is summed up as "*anga-fakatokilalo*" (to act in a milder manner), "*fakavaivai*" (to give in), "*faka'aki'akimui"* ("self-derogatory manner") and "*mo'ulaloa*" (submissive or subservient) (p. 40). Baker (1897) also provides the Tongan meaning for *lototō* as "honesty" (p. 143); honesty is "*angatonu*" (p. 6) and (p. 43).

A clear example of *lototō* is clearly explained in the History Section 2.4. The attendance of the first Queen of Tonga late Queen Salote Tupou III at Queen Elizabeth II's coronation in London UK in 1953. The late Queen rode in an open carriage during an outpouring of rain to be similar with the audiences that were standing outside watching the coronation. The act of the late Queen expresses real characters of Tongans - *lototō, anga-fakatokilalo, fakavaivai,* and *angatonu*.

2.10.5 'Ofa

'*Ofa* means love (Niumeitolu, 2007) (p. 158), (Ketu'u, 2014) (p. 7), (Kalavite, 2010) (p. 34). In the Tongan hierarchical ladder, Bennardo (2008) defines *'ofa* as "giving, either giving help (from higher to lower), or giving duty or respect (from lower to higher)" (p. 175).

Fairbairn-Dunlop (2015) highlights characters and values of '*ofa* in Tongan ways of living such as: '*ofa* implies "self-sacrifice for the benefit of others"; '*ofa* is centralised on "a collective rather than an individualistic gain"; '*ofa* is centralised

in *fatongia* (obligations, duties, and responsibilities); '*ofa* involves with *'osikiavelenga* or doing the utmost or wholeheartedly or giving it at all; '*ofa* reveals "*fevahevahe'aki* (sharing)". (*Fevahevahe'aki* or sharing is proved by the act of sending money to Tonga to support families and to assist in migration from Tonga to Aotearoa). The author further stated that '*ofa* encompasses fundamental elements such '*ofa* '*Otua* (love God); '*ofa famili* (love parents and family); '*ofa fonua* (love the land that provides nourishment) (p. 16 - 17).

Fairbairn-Dunlop (2015) points out that children in Tonga were brought up in traditional life to grow up with '*ofa* and understand the significance of cultural values. Wherever places around the world they go – they always keep Tongan values in their minds and hearts. The author further stated that "these values connect them back to the homeland of Tonga" (p. 17). The combination of fundamental elements of '*ofa* '*Otua, 'ofa fāmili, 'ofa fonua* and the connection (or '*ofa*) to homeland mentioned by Fairbairn-Dunlop (2015) can be related to the concept of Sea of Red (SoR).

Sea of Red (SoR)

Previous descriptions and stories about the Red Sea or Sea of Red (SoR) in this context, is referring specifically to Tonga. SoR became eminent in 2011's Rugby World Cup held in New Zealand. Tongan supporters were dressed in red, together with flags and banners to support players.

In 2011, NZ Herald (2011) reported that:

> "As many as 7000 supporters were at Auckland Airport when the Tongan rugby team,'Ikale Tahi, arrived yesterday afternoon.
>
> The car park was a sea of red-and-white, with thousands of cars decked out in Tongan flags of all sizes" (NZ Herald, 2011) (paragraph 1 and 2).

Since the 2011 Rugby World Cup, the proliferation of SoR became more popular, especially in New Zealand, where major competitions took place akin to the 2017 Rugby League World Cup, 2019, All Blacks vs Tonga, 2019 rematch between Kiwi vs Tonga, and 2019 historical match between Australia vs Tonga. SoR is not specifically involved in the game field but encountered before and after games in public places, airports, Tonga, New Zealand, Australia, UK and the US.

Affirmation of SoR, evidenced by the overcrowded Tongan supporters, covered Hamilton's FMG Stadium, Auckland's Mt Smart Stadium and Auckland's Eden Park Stadium during respective games.

The SoR (Sea of Red) signifies the *loto 'o e Tonga* (the heart of Tongans). *Loto 'o e Tonga* is proved by *lototaha* or one mind (Baker, 1897) (p. 143). Morris (2009) translates *lototaha* as "of one heart" and sets an example of *lototaha* in terms of the relationship between the players and coach. To achieve the *lototaha*, both coach and players "are praying together, eating together, and *mohetaha* (camps or literally "sleeping together" before games)" (p. 29).

Figure 16: Sea of Red at Mt Smart Stadium in 2019.

(Photo: Siuta Laulaupea'alu, 2019)

In November 2019, the first time for Tonga to play against Australian Kangaroos, the world rugby champions, in a memorable match at Auckland's Eden Park Stadium. A great historical win, 16 – 12, over Australia. *Figure 16* is a photo taken by the author (Siuta Laulaupea'alu) during the historical win, and to produce

evidence of SoR at Eden Park. In one week before Tonga's win, another record for Tonga after stunning Great Britain in Hamilton's FMG Stadium. Simultaneously, in 2017, another story made headlines after Tonga knocked off the New Zealand Kiwis during the World Cup. All these stadiums were covered by most Tongan supporters being dressed in red.

Tongan top rugby league players were born and raised overseas, mainly New Zealand and Australia, designated to represent the Kangaroos and Kiwis teams but players declined and chose to represent Tonga. In this instance, the refusal of the players to accept these opportunities, despite the high pay-rate, simplifies the love of players to represent the homeland of Tonga, the origin of parents and grandparents. According to Fa'avae (2020), the refusal of Jason Taumalolo and Andrew Fifita (both professional players) to play for their birthplaces (New Zealand and Australia) was an "indicator of their commitment to honour their parents' inheritage and homeland" (p. 77).

Money is not an issue for Tongan players. Fox Sports (2019) states the dollar value of each player to play for the State of Origin game was AUD $30,000 per match. Stuff (2017) confirms a list of key rugby league players (Siua Taumalolo, David Fusitu'a, Manu Ma'u, Andrew Fifita and Jason Taumalolo) denied playing for New Zealand Kiwis and Australian Kangaroos but played for the Mate ma'a Tonga (MMT). RNZ (2019a) reports about Tevita Pangai Jr denial to play for the 2019 New South Wales State of Origin games against the Queensland team. This Brisbane Broncos rugby league star chooses to play for MMT despite the potential payday of AU$90,000 for three State of Origin games.

Furthermore, TVNZ (2019) reports the payment given to the MMT players after the match against Kiwis in June 2019. MMT players were paid NZ$2,500 each by the Rugby League International Federation (RLIF) and then the GoT topped it up to NZ$5,000 plus a weekly allowance of NZ$600. Stuff (2019b) clarifies Kiwi players receive $5,000 each per test match compared to $20,000 received by Australian players.

Tonga's senior players clarify the reason to play for Tonga is not money or fame but to represent the cultural heritage. Stuff (2019b) states that:

> *"For the players, it's not about money or fame. It's about representing their heritage and growing the Pacific game on the global stage. To do that, they need to be taken seriously like the tier one sides, according to several senior players"* (Stuff, 2019) (paragraph 1 and 2).

Mate ma'a Tonga (MMT)

According to Fa'avae (2020), *Mate ma'a Tonga* literally means or *Die for Tonga* (p. 76). It is an old theme that worked for a long time in Tonga but became popular when the Tongan National League team was named after *Mate ma'a Tonga*. Tonga College is a government male boarding school established by a joint effort between King Siaosi Tupou 1 and Rev Shirley W. Baker in 1882. Tonga College's motto is *Mate ma'a Tonga* and has still existed since 1882 (DBpedia, n.p).

The philosophy of *'Sea of Red*' (discussed in the last section) was deployed by the Tongan rugby league players to abandon the financial benefits of playing on foreign teams but representing Tonga is like MMT. The MMT relates to the love of country or love for Tonga even though the players resided abroad but love Tonga for their homeland. Fa'avae (2020) refers to the eagerness of the players to play for the *Mate ma'a Tonga* team was "predominantly based on their affiliation and strong connections with their kin" (p. 77). In this context, MMT is referred to '*ofa fonua* (love the land of Tonga), *faka'apa'apa mo talangofua 'a e fanau ki he ngaahi matu'a* (respect and obedience of children to parents), *lototaha* (of one heart) and *ngāue-fakataha* (team work).

Mate pē Tonga he ngāue 'a e Tonga' (Tongan-kills-Tongan)

A well-known Tongan *kanaga* is pronounced as *Mate pē Tonga he ngāue 'a e Tonga* (Tongan-kills-Tongan) (TkT). *Kananga* is known as "A cant word or saying; or a proverbial expression" (Rabone, 1845) (p. 139). Unfortunately, no record or source confirms the originality of this *kananga* but it is very popular in Tonga and overseas.

TkT is not related to physical war or fight to cause death. It is a metaphoric twist of meaning to set up plans to deceive others. An old style of misleading locals to gain benefits from others, it is still popular today both in local communities and Tongans overseas. For example, TkT, a businessman in the village who earns a lot of money. With the idea of *Lotokovi*, (cantankerous or ill-will (Baker, 1897) (p. 11) (p. 45)) or

evil-spirited mind for the businessman's wealthiness, families and friends set up evil plans to borrow money with a verbal agreement for a precise time to clear the debt. Because of the *falala* (trust), the businessman agrees to assist with the borrowers and give the money. As soon as the money is due to be paid back to the owner, the borrowers run away and no longer repay the money. A difficult decision remains for the businessman and he finally agrees to take no further or legal action to recover the money. The main reason is the borrowers are close friends and near family members. A long-standing rumour for the businessman's family if legal action is processed. In the end, the evil-mind set up is achieved, the money lost, business is *mate* (no longer operational) and, therefore, the business owner is back to the same level as other Tongans.

In this instance, the idea of *Mate pē Tonga he ngāue 'a e Tonga Tonga* (Tongan-kills-Tongan) (TkT) ie relative to the setup of scammers to victimise innocent internet users. The concept of TKT is either a defensive or an aggressive technique. For example, people were previously victimised by scammers and are these victims assisting other Tongan by sharing their stories and experiences with these scams? Or, the victims will try to defraud the people to be trapped in the same issues.

2.11 Church and Religious Belief

According to Ketuu (2014), the church in Tonga is one of the most powerful institutions in the society and the church minister (*faifekau*) is "held in very high" (p. 83) respect. At the beginning of chapter two, Tongan proverb, there is a discussion about the word *mala* (bad luck) and the outcome of *mala* is *mala'ia* "misfortune for wrong doing" Poltorak (2007) (p. 16).

Poltorak (2007) tells a story of a case in Vava'u Tonga. This case proved the power of the People of God (PoG) and the result of opposing the PoG. Disrespect to the PoG produces *mala* and leads to *mala'ia* and ends up in death. A *faifekau* (church minister) in one of the villages was disappointed with a man. This man, with two other friends, took wood from the church boat shelter to light a fire near the beach before they went off fishing. In the sea, when these men were diving, a shark chewed the arm of the man who took the wood while the other two men remained unbitten. The arm of the man that was bitten by the shark was the side that *fua*

(carry) the wood from the church boat shed. The men's blood clotted and ended up in the deceased (Poltorak, 2007).

> "Everyone goes fishing knowing that if they do something wrong they will be bitten by a shark. Do something bad to the minister or to the Church, something will happen. The man had taken wood off the shed before, but hadn't confessed when the minister got angry about it" (Poltorak, 2007) (p. 18 - p. 19).

Further, the Christian belief of Tongans is based on the Good Friday and Easter Sunday concept. A process of the crucifixion of Jesus Christ on the cross on Friday and the coming back of Jesus to life after death on Sunday. The crucifixion and resurrection of Jesus Christ aimed to: *show the love of God; save the world; free the world from sin; pay the world's debt*. These four facts about the crucifixion and resurrection of Jesus Christs are summarised below.

To show the love of God: the death of Jesus on the cross is an act of love to save the world. "God is love" (Kristeva, 1987) (p. 5) offers His son Jesus Christ, "the crucified son of God" (Carson, 2013) (p. 12), (Levin, 2006) (p. 417), to die on the cross in order to save the world.

To save the world: Palmer (2008) states that "Jesus is the Saviour of the entire world" (p. 70), Jesus is "the Saviour of mankind who will come and judge the world" (p.72), and "Jesus as the Christ their Lord and Saviour" Brown (2008) (p. 3).

To free the world from sin: Finlan (2011) confirms that "Christ died for our sins" (p. 9) and "Christ's death atoned for man's sins" (Brown, 2000) (p. 3). Thompson (1942) says that "Jesus frees us from sin" (p. 3) and:

> "Jesus Christ not only died on the cross and rose again, so that we may be forgiven of our sins, but also that we may have power over our sins; so that we may have power over the devil, who tempts us to sin in the sight of God" (p. 3).

To pay the world's debt: Brown (1996) states that people on earth were supposed to be dead because of sins but Jesus was nailed "to the cross [and our] debt is paid in full" (p. 2). Additionally, Edwards, Gabel, and Hosmer (1986) mention that Jesus

Christ "spoke seven times from the cross [before] Jesus passed away" (p. 13). The memory of the death and resurrection of Jesus Christ or crucifixion on Friday and resurrection or emergence of Jesus from the tomb on Sunday is regularly immortalised in Tonga every year.

Edwards, Gabel, and Hosmer (1986) further discuss the crucifixion and death of Jesus Christ.

> At about 3 PM that Friday, Jesus cried out in a loud voice, bowed his head, and died. The Roman soldiers and onlookers recognized his moment of death.... The soldiers broke the legs of the two thieves, but when they came to Jesus and saw that he was already dead, they did not break his legs (p. 13).

Also, Jesus was crucified in the cross and on the third day Jesus was resurrected and restored to life. Brooks (2017) confirms the resurrection of Jesus Christ, the Son of God, and after three days in the grave, Jesus rose from death: "….the Empty Tomb, fulfils the Resurrection predictions, and probably belongs to the same layer. It depicts Jesus' burial and his bodily Resurrection after three days" (p. 84).

Good Reads (2019) brings a quotation from Bishop Lesslie Newbigin of England about the resurrection which says: "The resurrection is not the reversal of a defeat but the proclamation of a victory" (paragraph 6). Bible in One Year (2018) also quotes the same words commented by Bishop Newbigin that:

> The resurrection was not the reversal of a defeat but the manifestation of a victory. The cross was not a defeat. Rather, taken together, the cross and resurrection are the greatest victory to have taken place in the history of the world. It is a victory that has huge implications for our own lives, our society and the future of this world (Bible in One Year, 2018).

As the majority of Tongan locals are Christians, "ninety percent" (Niumeitolu, 2007) (p. 7), the people of Tonga, without any doubt, believe there is life beyond-the-grave. After human life on earth, Heaven is the next new home for Christians to stay eternally with God. Siegel (1980) agrees there is a new life after death: "…..when a person dies, a swarm of highly charged energies deserts the body and

goes out into space, entering another cycle of life….. Life after death was a reality" (p. 911).

All the hard work, commitments and religious activities conducted by Tongans are focused and targeted to accomplish the second life, to receive eternal life and to be accompanied with God in Heaven.

Bible in One Year (2021) quotes about the future of the people on the earth that:

> Death is not the end: 'By his power God raised the Lord from the dead, and he will raise us also. Not only can you be sure that one day you will be raised to eternal life, but through Jesus you can also be assured that you can appear with confidence before the judge of all the earth sanctified and justified (paragraph 20).

2.11.1 Christianity in Tonga

UCG (2004) describes Christian as the people who believe in Jesus Christ, the "crucified son of God" (Carson, 2013) (p. 12), (Levin, 2006) (p. 417) the Messiah (Whitsett, 2000) (p. 681) and "Jesus Christ is our Lord" (Whitsett, 2000) (p. 673). Another impression of Christianity is the concept of being born again. Born again is about the regeneration of the spiritual life or the human heart by the Spirit of God (Compelling Truth, 2019). Dixon, Levy, and Lowery (1988) state that being born again is a "turning point in your life when you commit yourself to Jesus Christ" (p. 34).

Schaeffer and Heath (1982) express the view of Christianity. Christian holds the law of God as an objective standard. The law of God holds "as an objective truth apart from the will of man" [and] "the reformation was in part the clarification of the true basis of society and law: the Word of God" (p. 2). The Word of God is described by Thompson (1942) as: "…. the source of light, truth and power, for those who seek its meaning and apply it to their life. Jesus Christ is the Word made flesh, and we seek to follow him" (p. 1).

In Tonga, King George Tupou 1, the 17th Tu'i Kanokupolu commenced on 4th December 1845, the inherited monarchy line today, was baptised as a Christian in 1831. Not only has the King accepted Christianity, but George also made changes to Nuku'alofa to become the capital of the realm in 1845. Further, on

4th November 1875, the adoption of the constitution and Tonga formally became a Kingdom (Find a Grave, 2012).

George is well known for the performance of *Tuku Fonua ki Langi*, the act of giving of Tonga to the sky / God. Tongan officials urged the King to hand over Tonga to be looked after by a wealthy overseas nation such as France or Great Britain. However, the King picked up a handful of soil from the ground and lifted it to the sky. The king shouted, "God and Tonga are my inheritance" (*Ko e 'Otua mo Tonga ko hoku Tofi'a*) which became the nation's motto (Niumeitolu, 2007) (p. 8 – 9). Tonga is handed over to be fully controlled and taken care of, by God.

Figure 17: King George Tupou 1 (1797-1893)

Source: (Find a Grave, 2012)

Figure 17, the image of King Siaosi Tupou 1 (George Tupou 1) named after King George 111 of England, is well known as the initiator of modern Tonga (Find a Grave, 2012).

According to Niumeitolu (2007), Tonga is always known as "*ko e fonua lotu 'e ni*" or "this is a Christian nation" (p. 7). Also, Kalavite (2010) provides other evidence that 98 percent of the Tongan population belongs to "Christian church" (p. 45). The connection of Tongans to Christianity is reflected in the colours (red and white) and the cross sign in the Tongan flag. The Red Cross signifies the blood of Jesus Christ

when Jesus was crucified and hung on the cross. The white colour implies the rise of Jesus from death in the grave to provide salvation and "purity" to the world (Kalavite, 2010) (p. 45).

2.11.2 Churches in Tonga

Tonga Department of Statistics (2014) summarises the portion (percentage) of churches. Top five churches (see *Table 7*) with the highest number of local members (36 percent) belong to Free Wesleyan Church (FWC). A total number of churches exceeds 20 congregations with well-known churches. Included churches in *Table 7*, are: Tokaikolo Christian Fellowship, Anglican, Seventh Day Adventist, Constitutional church of Tonga, Gospel, Bahai, Hindu, Assembly of God, Islam, Buddhism, The Salvation Army and Pentecostal Denomination (p. 3).

Table 7: Tonga Religions

Church	**Percentage (%)**	**Members**
Free Wesleyan Church	36	36,592
LDS Church (Mormons)	18	18,554
Roman Catholic	15	15,441
Free Church of Tonga	12	11,863
Church of Tonga	7	6,935

A new church is known as 'Mo'ui fo'ou 'ia Kalaisi' which was recently established in 2013 as a result of the separation of new church members from the original church of the Tokaikolo Christian Fellowship (Kaniva Tonga, 2013). In Tonga, every village owns more than one church with large buildings owned by churches. One church can own more than one building: hall, church, and accommodation for church ministers and stewards.

"Jesus is the temple in whom God dwelt in all his fullness. Church is not an organisation you join; it is a family where you belong, a home where you are loved and a hospital where you find healing" (Bible in One Year, 2019). Clowney (1973) explains that the purpose of establishing the temple is to be a meeting-place between God and the people.

Church Ministers and Stewards are assigned by the church conferences to) to serve the Word of God in local villages and overseas (Fiji, Samoa, Niue, New Zealand, Papua New Guinea, Japan, Australia, the United States, and the United Kingdom. In Hamilton New Zealand, there are Tongan churches such as Free Wesleyan Church, Free Church of Tonga, Latter Day Saints LDS Church (Mormons), Roman Catholic, Maama Fo‘ou and Tonga Methodist Church. Some of the church leaders were originally Tongan born who are controlled from respective Head Offices in Tonga.

Figure 18: St. Joseph Cathedral, Vava'u, Tonga

Source : (Dreamstime, 2014)

Figure 18 is a Catholic Church building located in the heart of Neiafu the capital of Vava’u.

A memory of late Reverend Sione Kami is honoured by Papuans for a meticulous gentleman to bring the light of God to shine upon the people of Papua New Guinea. A church building called ‘Rev. Sione Kami Memorial Church’ was built and located in Port Moresby, Papua New Guinea (Local Prayers, 2012) to record the long term services and good works of this good shepherd. Reverend Kami has passed away and his body was buried in the homeland of Tonga.

2.11.3 Misinale and church obligations

Ketu'u (2014) states that "*fakaafe* and *misinale*" are the two major religious tasks of Tongans to show appreciation to God for his "love and provision" (p. 81). God loves the world and provides life, food, money, freedom, air, light, warmth and so on. In appreciation, Tongans pay back to God through church donations and other church activities. PNW (2015) describes *misinale* as the annual ceremony of offerings of money to the church by Tongans. Evans (1999) also describes *misinale* as contributions and are "gifts to God [and are part of] ongoing relationship between God and the givers" (p. 154).

Table 8: Cultural and religious expenses

Item	Amount (TOP$)	Reference page
Traditional birthday ceremonial	TOP $29,100	(p. 92)
Traditional wedding ceremonial	TOP $50,700	(p. 94)
Traditional nuclear family funeral	TOP $42,000	(p. 96)
Church obligations	TOP $25,000	(p. 98)

Source: (Ketu'u, 2014 – approval granded in September, 2019)

Figures provided by Ketuu (2014) in *Table 8* reveal the average financial spending on cultural activities and religious obligations in Tonga. Misinale plays central roles as part of the money is contributed to building. Many local church buildings were built by the church donations and fundraisings. One church, Tokaikolo Christian Church, donated an estimated one million pa'anga in one year. Another instance happened as a member of a family passed away and the family donated TOP$20,000 toward the annual misinale in remembrance of the lost family member (p. 166).

Item	Average estimated cost (TOP)
Misinale or annual church donation (range from 1000 to 10,000)	5,000
Fakamānatu or acknowledgement of a deceased member of the church (could range from 1,000 to 10,000)	5,000
Sapate faka-Me or White Sunday	500
Sapate Fa'ē or Mothers' Sunday	500
Sapate Tamai or Fathers' Sunday	500
Faka-Sepitema or Women's September Day	500
Fakaafe kilisimasi or preparation of Tongan feast for Christmas church service	3,000
Ngaahi pola konifelenisi or preparation of Tongan feast for church annual conference	3,000
Fakaafe faka'osita'u or preparation of Tongan feast for End-of-year and New Year church services	3,000
Fakaafe uike lotu or Feast for the New Year Prayer Week	3,000
Fund raising for various church activities	1,000
Total	**25,000**

Figure 19: Average annual church expenses in Tonga

Source: (Ketu‘u, 2014).

A summary of expenses for church obligations and services is also broken down in more detail (see *Figure 19*). Spending on *misinale* was TOP $5,000 (20 percent) and the remainder is for other expenses. More information about the figures in the table shows in the next section.

Issues of Misinale

In the occasions of *misinale*, wedding, birthday, funeral and other cultural activities, the rumour of *fakavahavaha'a* or competition is well-known there (Ketu'u, 2014) (p. 78). In the church, members and families compete for who or which family gives the highest amount of money in the *misinale*. In terms of *fakavahavaha'a*, the pressure of being announced to be the top giver or the highest amount of money donated in the *misinale* is only to be famous and praised by the church leaders and community. Truthfully, the actual giving is not coming from the heart. At any stage where the saving (money) for the *misinale* is insufficient, or a family hears that the neighbour has more money, then the family tends to look for another source of

funds to top up existing savings to beat the neighbour and lead the highest donation amount.

An average household income for Tongans is "22,000 pa'anga" yearly (Ketu'u, 2014) (p. 198) and the annual spend on church obligations is TOP $25,000 pa'anga. Obviously, the total amount of church obligations is higher than the average household income. The result of the deficit margin (surplus of TOP $3,000) is reflected in continuous lending from the banks. Ketu'u (2014) confirms that 50 percent of Tonga Reserve Bank's personal loans were spent on birthdays, a wedding, funeral and *misinale*. And most of these loans' purposes are aimed for church obligations.

Sunday services and Taboo

Work is prohibited on Sunday. Except for the Ministry of Police, Ministry of Health, Ministry of Defence, and some tourist-related services are in full operation. Government Ministries, shops, airports, gas stations, taxis, nightclubs, farm works, fishing, and other public services are closed on Sunday. Starting on midnight Saturday to midnight Sunday (24 hours), no one is allowed to break the law of Sabbath. Sunday is dedicated to God. Early in the morning, around 4am, loud noises of *lali* (wooden drums) and bells wake up Tongans to get out of bed and be ready for early morning church services at 5am – 6am. The main services are held from 10am – 11am and 4pm – 5pm. After the main service in the morning (10am – 11am), youth and children continue to *lautohi faka-Sāpate* (bible study). Other activities, such as youth and church meetings, are held in the rest of the evening until 10pm – 11pm or midnight.

> The Sabbath Day shall be kept holy in Tonga and no person shall practise his trade or profession or conduct any commercial undertaking on the Sabbath Day except according to Law; and any agreement made or witnessed on that day shall be null and void and of no legal effect (Latukefu, 1975), (Ketu'u, 2014).

2.11.4 Religious belief of Tongans

The London Missionary Society (LMS) had a profound influence in Tonga. Although the first attempt of the former LMS failed, but Thomas and Hutchison, two Wesleyan missionaries, successfully landed in the village of Ha'atafu in 1826.

Taufa‘ahau or King George of Tonga was required to prove the reality of the new church and God. Pita Vi was the first Tongan preacher to serve the Words of God in the Ha‘apai Group of Islands (Tu'ipulotu, 2013) (p. 19). King George was accompanied with Pita Vi on a sea voyage from Pangai Island (the capital of Ha’apai) to another island of Ha’ano. Taufa’ahau ordered the crews to throw Pita Vi into the open sea to be eaten by *Taufatahi* (a god of sharks). If *Taufatahi* devoured Pita Vi then the new church or God is untrue. During the King royal *taumafa kava* (drinking kava) in Ha‘ano Island, Pita Vi arrived safe, unbitten, and untouched by Taufatahi (Tu'ipulotu, 2013).

Passage (2016) further clarifies that: “In 1830 and 1831, Missionary John Thomas and his Tongan assistant, Pita Vi, converted Taufa’ahau – one of the claimants to the Tui Kanokupolu line – and Christianity began to spread throughout the islands” (Passage, 2016) (paragraph 8).

Kalavite (2010) confirms that religious belief in Tonga is based on the Holy Trinity. The doctrine of Trinity is “God in three persons: God the father, God the Son and God the Holy Spirit” (p. 45). Further, Kalavite (2010) extends that: “The Tongan Christian belief is that God is the source of all good things and God blesses those who truly believe in him and live the Christian faith. God has the power to protect and empower people. Every blessing is from God who rewards those who believe and follow the teachings” (p. 45).

One case highlights the strength and power of the religious belief of Christianity. The termination of Former Wallabies rugby star Israel Folau by the Australian Rugby Football (ARF) delivers strong messages to Christian followers. Although this Tongan inheritance Australian born rugby superstar’s four-year A$4 million contract has been terminated by the ARF, Folau insists on the truth and personal belief about God. Despite an offer of one-million-dollar settlement from ARF, Folau makes clear that money is not the main issue but to express Folau’s personal love and belief in God (Stuff, 2019a).

The latest update about this case from Pink News (2020) on April 2020 summarises that:

- In December 2019, “Rugby Australia issued an apology for any harm caused to Folau as part a settlement over his sacking for anti-gay comments” (Pink News, 2020).
- Folau reached an undisclosed clearance with the New South Wales Waratahs and Rugby Australia, “bringing to an end his $14 million wrongful dismissal lawsuit” (Pink News, 2020).

2.12 Chapter Summary

Some of the questions in the questionnaires were drafted based on the information discussed in this chapter. This means this research project is not limited to cybersecurity theoretical and technological platforms but to explore more on other non-cybersecurity features such as human, culture, economics, hierarchy and religion in Tonga.

This is an opportunity to *kilala*, (“to uplift or revive”) (Churchward, 1959) (p. 264), the ancient theme of the Tongan proverb *Tala ke i Kapa na’a ke too ki Mala* and to theorise the meaning behind this proverb to be a cybersecurity awareness and prevention tool. In the meantime, there is another chance to revitalise and practice some of the ancient Tongan concepts. The Tongan concepts are *Mate pē Tonga he ngāue ‘a e Tonga* (Tongan kills Tongan), *Tahi Kulokula* (Sea of Red), *fakavahavaha‘a* (competition) and *Kavei-koula ‘a e Tonga* (Tongan golden values) such as *faka‘apa‘apa*, *lototō*, *tauhi-vā*, *mamahi‘ime‘a* and *‘ofa*. These concepts are combined together with human and cultural features to be the major fundamental areas of this research.

CHAPTER THREE

3. LITERATURE REVIEW

3.1 Introduction

Numerous academic research projects that have been undertaken in the area of cybersecurity are summarised in this section. Most of the scholars' research findings assist in developing new ideas to guide this thesis. They assist in identifying cybersecurity gaps and try to avoid duplication of other scholars' original ideas. Research findings have also been reviewed to understand the ICT trends, when shifting the focus from developed states to developing nations, and how it is impacting the South Pacific Islands (SPI).

One of the major impacts discovered in these academic research findings is the rapid coverage and growth of cybercrimes and cybercriminals in the SPI. Lessons from these kinds of literature assist with the formulation of appropriate cybersecurity approaches and set-up of effective preventative and awareness programmes that are relevant for SPI. Also, the pieces of literature facilitate the set-up of appropriate questions for the survey participants. These questions will provide new answers and new findings that no other scholars have discovered in their previous academic studies.

The Literature Review Section is divided into six main divisions. The primary section discusses cybercrime cases and their global impacts. Other sections focus on defensive mode; on how to set technical, cultural and social approaches to defending against online frauds. The last three sections summarise the rise in the number of cybercriminal cases and the impact of ICT in developing nations and the SPI and recent COVID-19 impacts. Details of the main sections are as follows:

- Section 3.2: What is Cybercrime
- Section 3.3: Offences and Cybercriminal Cases
- Section 3.4: Cybersecurity Defences
- Section 3.5: Cybercrime in Developing Nations
- Section 3.6: Cybersecurity in the SPI
- Section 3.7: COVID-19 Scams

3.2 What is Cybercrime?

Karl de Leeuw and Jan Bergstra (2007) attempt to elucidate distinctly the word crime and cybercrime. A crime involves "engaging in conduct that has been outlawed by a particular society with acts of theft, rape, murder, assault and vandalism. [Cybercrime is] "the use of computer technology to engage in socially outlawed conduct. Criminals use guns to commit crimes while cybercriminals use ICT technology (e.g., computer) to engage in outlaw conduct" (p. 705). Examples of these cybercriminal cases are extortion, stalking, theft, fraud, and other varieties of crimes. Karl de Leeuw and Jan Bergstra (2007) conclude that the greatest cybercrime today is the "migration of real-world crime into cyberspace" (p. 706).

Futter (2018) briefs a presidential debate between Donald Trump and Hillary Clinton in 2016 and these are quoted words spoken by Donald Trump that: "cyber was one of the biggest threats facing the United States, and that the US must get very, very tough on cyber" (p. 201).

Ottis and Lorents (2010) prefer the term cyber to "almost anything that has to do with networks and computers, especially in the security field" (p. 267). Clough (2015) gives a tripartite classification based on the US Department of Justice to clarify computer crimes into three categories. These are:

1. Computer-crime which is crime involving a computer or computer network to target criminal activity, e.g., malware, hacking and DoS attack.
2. Computer-facilitated crime as the use of a computer as a tool to commit a crime, e.g., fraud, stalking, child pornography and criminal copyright infringement.
3. Computer-supported crime is the use of a computer in a related aspect of crime and afford evidence of the crime, e.g., found address of suspected murder in a computer, or a conversation or phone record between suspect and victim before a homicide (p. 10).

Cybercrime has multiple facades and occurrences in different scenarios which then result in conceptual complexities. Yar (2005) has informed the primary issue for analysing cybercrime is the non-presence of a consistent up-to-date definition. The tracing of cybercriminals is a critical problem and very complicated in comparison with conventional crime, as there is no fingerprint, according to Li Zheng and Chen (2006).

A fingerprint is a mark or dip of the individual's fingertip that appears on a surface and can be used to identify a person from the pattern of lines and whorls on the fingertip. Evidence of fingerprints are available and can be collected from traditional crime as criminals are able to visit and touch the criminal site. In terms of cybercrime, cybercriminals stay in their own room and set up connectivity with the outside world.

Online fingerprint takes a complex process to be identified. The fingerprint is stored in a database and the usual authentication process (for example, logging into mobile phone using thumb) takes an extra second in trying to match fingertips of the thumb with the database fingerprint. As soon as the fingerprint matches with the database, the system allows access. No match and no access to the system. Liu, Jiang and Kot (2007) clarify this process is "more complex than the authentication" (p. 1795).

Le (2009) requires developing an efficient system to minimise the searching time in the database. Search performance is matched in a small database, but it requires an effective fingerprint indexing scheme for a large database. Hashing is one of the traditional techniques to minimise the searching time. This practice is only related to the authentication process but not related to identifying cybercriminals' online fingerprints.

This behaviour makes it hard for the cybersecurity's investigators to obtain evidence such as fingerprints, as discussed above by Li (2006). Joakim Kävrestad (2017) clarifies that most people get their own computer systems and so it is easy to commit cybercrimes from the privacy of their own homes. Loader and Thomas (2013) further extend by giving an example that using a computer to cheat someone is "no different than the use of telephone or face-to-face conversation to deceive someone" (p. 6).

Gordon and Ford (2006) provide a definition of cybercrime, from the Cybercrime Treaty of the Council of Europe report, as the offences "ranging from criminal activity against data, to content and copyright infringement" (p. 14). It also includes unauthorised access, fraud, cyberstalking and child pornography. The Prevention and Control of Computer-Related Crime (PPCCRC) of the United Nations Manual defines cybercrime as forgery, fraud and unauthorised access (Gordon & Ford, 2006)

Li, Zheng, and Chen (2006) generalise the meaning of cybercrime to include computer hacking, network intrusion, internet fraud, spreading of malicious code and cyber-privacy. They further extend this to include the methods of communication used by Al Qaeda and Osama bin Laden for terrorist attacks, which have been through online message networks (Li et al., 2006). Blanco Hache and Ryder (2011) defines cybercrime as the successful transformation of "traditional crimes into more modern ones using the internet" (p. 35).

Finklea and Theohary (2012) provides a conceptualising process to further simplify the definition of cybercrime by using key-question words of who, where, what and why (4W). For example: Who is involved in fraudulent actions? Where do the malicious acts happen? What technologies are involved? Why are malicious events started?

By using of 4W (who, where, what and why), the meaning of cybercrime is expanded to cover other parts such as human behaviours, technical sites, reasons, place, and types of cybercriminals. In conclusion, cybercrime is illegal activities related to using network-or computer-related devices to gain profit are conclusively belong to cybercrime or cybercriminal.

3.2.1 Classifications of cybercrime

Gordon and Ford (2006) have split cybercrime into two separate types. Type 1 cybercrime is "mostly technological in nature" and Type 2 cybercrime "has a more pronounced human element" (p. 13).

Type 1 generally deals with a discrete instance or single event such as user tries to open, read, and reply to the email sender. To reply to a fake email initially opens the gateway for a cybercriminal to generate a fraudulent action by misdirecting the user to click on a link resulting in downloading key logger or a Trojan virus. Cybercriminal then uses user information to defraud the user. These types of cybercrimes are known in phishing attempts, identity theft, bank fraud, hacking, virus, manipulation of data, and other e-commerce fraud derived from stolen credentials (Gordon & Ford, 2006).

Type 2 cybercrime refers to activities such as child predation, cyberstalking, harassment, blackmail, extortion, corporate espionage, stock-market manipulation

and plans to carry out terrorist attacks online. One characteristic of Type 2 is where the programs are “not fit under the classification crimeware” like a conversation taking place using Instant Message clients or transfer of files using FTP protocol (Gordon & Ford, 2006).

Segal (2013) provides a global example of cyber-instability, which was a mistrust between the United States and China which causing three main instability issues: “offence advantage, attribution and speed of conflict” (p. 41). An example of an attribution issue relates to a network attack and the major issue is the attacker is masked, difficult to detect or locate the physical address, a complication of attacking from a proxy server, and unable to respond promptly. Child cyber-instability associates when two individuals start building a relationship on the internet without facing each other but they both start to share emails or online chats. One user who is the innocent party might become suspicious as the other user is not keen to meet face to face or refuses to share contact details. Meanwhile, the cybercriminal starts posting false statements online or sends emails to frighten the innocent user. The relationship is reversed as the innocent user’s initial engagement was for a genuine purpose, but the cybercriminal is targeting to gain profits from the innocent user. When the innocent user becomes frightened and concerned about being secured, the case may be referred to the police to act. The emotive action of the cybercriminal towards the innocent user is known as cyberstalking (Gordon & Ford, 2006).

3.3 Offences and Cybercriminal Cases

3.3.1 What is online scamming?

Elliott (2011) refers to the word scam as *rip-off* or *bad-deal* (p. 15). A rip-off involves deception. For instance, a shady second-hand-car dealer may rip customers’ off by rolling back odometers of cars and sell out at high prices. Bad-deal deals with overpricing or selling items at high prices with inferior (poorer) quality (Elliott, 2011). Geis (1991) states that scam is a common consumer-crime known as a “bait and switch tactic”, “evil grandeur” (high rank) and “white collar crime” (p. 8). C. Cox and Whalen (2001) refer to grandeur is “considered a metaphysical evil” (p. 4). Shover, Hochstetler, and Alalehto (2013) refers street-crime is involved with violence and threats, “white-collar crime is distinguished by

perpetrators' use of concealment, deceit or guile; white-collar violates trust" (p. 477). Finally, Vadera and Aguilera (2015) define white-collar crimes as "illegal and unethical actions by agents of an organisation" (p. 21).

More information from other websites are included in order to extend the meaning of the word scam. Computer Hope (2020) refers scam to any related fraudulent scheme or business that takes goods or money from an innocent person. Various types of scams target to steal people's property, information and money. Here are the common scams: phishing, auction fraud, donation scam, catch fish, cold call scam, 419, chain mail and online survey scams (Computer Hope, 2020).

Schaper and Weber (2012) describe scam as a "form of dishonest action, based upon an invitation to participate in an activity" (p. 333). Victims are induced, misled and encouraged by scammers to voluntarily surrender their valuable resources to scammers. The philosophy behind rip-off and bad-deal can be transformed from a business deal to other areas including cybercrime. In cyberspace, *rip-off* and *bad-deal* can be referred to as deception, fraud, trick, induce, lie, mislead, encourage, convince to believe and dishonesty. All these characteristics are the main tactics deployed by the scammers to mislead the innocent internet users. Scams display wide ranges in traditional crimes and become prevalent on the internet to form different forms of online crime. Schaper and Weber (2012) also classify different types of scams which are unrelated to the use of computer and the internet. These scams are as follows: false business valuation, phishing, dishonest advertisement listings, false directory, bust-outs, cramming, blowing, misleading self-employment projects and advance fee fraud. These scams can be classified in both traditional crimes and online crimes or online frauds. Blanco Hache and Ryder (2011) generalise online fraud as "deceptive behaviour conducted through the internet in an illegal manner. Financial and personal benefits are the major motivation for e-frauds" (p. 38).

3.3.2 Types of online scamming?

There are different types of online scams such as scam baiting, email spoofing and lottery scams. There are only four types of scams based from CERTNZ (2019) to be discussed in this section - Online Romance Scam (ORS), Money Scam, Social Media Scam (OMS) and Phishing scam.

Online Romance Scam (ORS): Whitty and Buchanan (2012) state that ORS became active in about 2008. Scammer tries to make an online relationship (through a dating website or social media) with the victim. Once the relationship gains trust between each other, the scammer asks for gifts, money and personal details to commit fraudulent acts. This scam is hard to identify as scammer often uses a fake profile. Between 1/4/2010 and 1/4/2011, "Action Fraud identified 592 victims of this crime in the United Kingdom. Of these victims, 203 individuals lost over £5,000" (Whitty and Buchanan, 2012) (p. 181).

Money Scam: this scam uses the get-rich-quick scheme to deceive innocent citizens. A get-rich-quick scheme is typical of fast money scheme or Ponzi scams (J. Cox & Macintyre, 2014) (p. 138). According to Moore, Han and Clayton (2012), the main concept behind a Ponzi scheme is that payments are paid to current investors from funds deposited by new recruitment members until insufficient funds are left and the scheme collapses. They also stated that "similar schemes have operated in the offline world for 150 years or more and are often called Ponzi schemes after a famous swindler in 1920s Boston" (p. 1).

Social Media Scam (OMS): Nadaraja and Yazdanifard (2013) list some of the opportunities and challenges of social media. The authors state one of the main challenges of using social media is trust. The building of trust between friends and families, such as accepting friends on Facebook, sharing information on social media and sending links on email, is based on trust and knowing each other very well. On the other side, OMS is involved in trying to build trust for fraudulent purposes. A scammer pretends to be someone who is very close and knows the victim very well. Normal tactics involve the scammer telling the victim that their money was stolen and they have no more funds available to return home. With good faith, the victim agrees to help and gives money.

Phishing scam: Phishing attacks have been predominant for more than 10 years (2008 - 2018) and are a current ICT threat to both individual users and organisations (Jayden Nowitz, 2018).

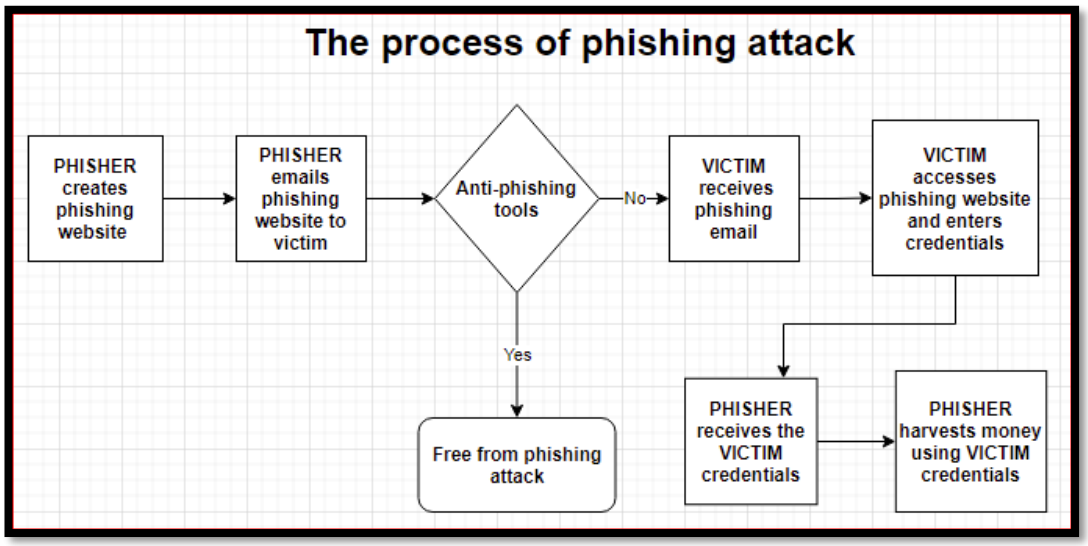


Figure 20: Phishing attack pathway

Source: Research Gate (2021)

Phishing involves the attempt to steal sensitive information. Scammers send emails or links to the victims, asking them to provide details, such as social security numbers, credit card numbers, passwords and usernames (see *Figure 20*). The emails or links look genuine and victims reply and provide the information requested. The scammers accessed and use this information provided for personal and financial benefits.

3.3.3 Phishing Attacks

Saberi, Vahidi and Bidgoli (2007) clarify that "phishing is a branch of internet crimes" (p. 311) and "phishing attack is a kind of identity theft" (p. 311). Identity theft relates to cybercriminal attempts to gain bank credentials from victims to steal money from their bank account. Mohammad, Thabtah, and McCluskey (2015) have produced a report conducted by Gartner Inc. in 2011. The report revealed that phishing websites cost an estimated $3.2 billion to the US financial-sector and around "3.6 million victims fall" in these phishing attacks (p. 11). Another report from Anti-Phishing Working Group - APWG (2016) shows that the total number of phishing attacks in 2016 was more than 1.2 million, which is an increase of 65 percent from previous years (Jayden Nowitz, 2018). Further, Lalitha and Udutha (2013) mention the "increase in phishing over the last few years has been a serious threat to the economy and global security" (p. 1733).

Phishing is like fishing in the sea where the fisher hooks the bait onto the fishing line with the intention of catching fish. The difference is the fisherman aims to catch fish but the phisher targets computer users to gain secret information (James, 2005). It is a form of identity theft with combinations of sophisticated attack vectors and social engineering techniques to reap financial information from innocent users (Garera, Provos, Chew, & Rubin, 2007).

Phishers rely on spoofed emails to persuade victims to respond back with the required information. Social networking websites are active tools used to distribute suspicious links to trap victims to click on phishing links or websites. Hong (2012) confirms most "phishing email-messages use social techniques rather than technical tricks to fool end-users" (p. 75).

Hong (2012) categorises the structure of the phishing attack in three main phases. The first phase involves the target victim receiving the bait. The second phase is where the victim tries to complete the suggested requirements in the phish message. (These requirements usually direct the victim to a fake webpage or install malware or the victim replies and provides confidential to the message). The third phase involves the monetising (converting to money) of the victim's stolen information.

Bergholz et al. (2010) agree with other scholars' views that most phishing emails target victims to gain confidential information and aim to withdraw money from financial organisations. Volkamer, Renaud, and Gerber (2016) brief about phishing by saying that phishing messages hook "a bait embedded in alluring text which entices the recipient to click. If they do click, it redirects them to a doppelgänger website" (p. 372).

3.3.4 User-behaviour and URL visual spot

Alsharnouby et al. (2015) inform that quick visual assessment of websites by users are not duly focused on the most reliable key indicators. Internet users normally want quick access to websites and often do not look carefully at spelling. If the internet users take time to have a second look that might help them to spot the illegitimate website. These characteristics or procedures are normal and likely to be a daily routine for internet users. On this point, Alsharnouby, Alaca, and Chiasson (2015) conclude that scammers are able to deceive internet users with "visual characteristics sufficiently believable to be accepted as legitimate" (p. 71).

Volkamer et al. (2016) informs that “phishers know that many users will not consult the address bar to check the URL” (p. 373).

The visual spot of the URL indicates the security and non-security of a website. A legitimate URL starts with a picture of a padlock in front of the https address. The last ‘s’ letter in the https stands for ‘secure’. This mean that data file is bound with a cryptography key or SSL (secure sockets layer) certificate. If the URL does not have a padlock picture or ‘s’ like http, then this website is not secured. Europol (2019) advises about online payment is to check the URL bar for the https and padlock and to choose and use a reliable mobile network connection for payment instead of public Wi-Fi.

Chomsiri (2007) states that https is a “secured communication channel more than http protocol” (p. 1). And, more e-commerce businesses are operated in the https protocol. Naylor et al. (2014) examine the traffic flow in https of 25,000 ADSL (Asymmetric Digital Subscriber Line) customers in Europe in 2014. The result shows https upload volume was 80 percent and download volume was down to 25 percent only. Naylor et al. (2014) conclude that https download “volume is accelerating” (p.1). However, Chomsiri (2007) concludes that hackers are enabled to attack the https. Man-in-the-middle attackers used some attacking tools such as SSL Dump, Sniffing, DNS and ARP Spoof to capture, decode and interrupt the secret information. “The interruption can be encouraged by using Static ARP at the switch and using ARP Watch to alert the administrator. More to the point, Anti-Sniff provides a function to scan a machine that is capturing information” (p. 5).

One of the Journal Articles, ‘Spot the phish by checking the pruned URL’, authored by Volkamer et al. (2016), mentions that technological prevention of phishing messages is impossible due to innovation and continuous technological changes developed by cybercriminals. A common phishing detection technique of Blacklists has struggled to stay current, and the number of attacks escalates each year. In 2013, the detection process took an average “28.75 hours to detect new phish website”. To decrease the number of phishing attacks’ success, the user should “consult the address bar to check the URL” (p. 373).

A major concern about the small size of the mobile phone and the rising in the number of mobile usages. Visual spot on the mobile phone by naked eyes for

legitimate URL becomes an issue due to small screen size. Identification of legitimate URL on the desktop device is not an issue as the screen is large and the URL can be easily spotted. The smaller the size of the screen, the harder it is to spot the URL. Some of the mobile phones (e.g., iPhone 6) display partial URL and are unable to identify whether the URL belongs to http or https.

3.3.5 Ransomware

Ransomware is a type of malware designed by cybercriminals to block users from accessing the computer system. Gazet (2010) combines malware and ransomware to define the meaning: "a ransomware is a kind of malware which demands a payment in exchange for a stolen functionality" (p. 77). Pathak and Nanded (2016) also describe the exploitation of ransomware in the computer system. Ransomware enters the system by an exploit kit or a portion of another malware's payload, searching for vulnerability areas and then "silently installs and executes in the malware" (p. 371).

Additionally, Trend Micro (2018) defines ransomware is a malware that avoids or prevents the user from accessing into the system. The computer system either locks the user's file or locks the system's screen and demands that a ransom be paid. Ransomware can be a scareware as it targets to deceive computer-users to visit malware-infested websites and finally end up with full demand from the cybercriminals for the computer-users to pay ransomware (Trend Micro, 2018). According to Richardson and North (2017), MacAfee Labs measure 1.2 million ransomware attacks, [and the FBI estimates that] ransomware generates approximately $209,000,000 in the first three months of 2016" (p. 13).

According to Pathak and Nanded (2016), there are two effective types of ransomware used to generate a huge amount of revenue, Locker Ransomware and Crypto Ransomware. Once the user's system is compromised, cybercriminals manage to control and then demand payment be made before they decrypt files/documents and allow the system to be operational. It is a traumatic experience as money must be paid first before the system returns to normal functionalities and the ransomware payment does not guarantee full access to the infected computer system. Locker Ransomware blocks the computer system, and the user is no longer able to access it. The cybercriminals use payment vouchers to demand payment

from the victim. Crypto Ransomware is used to encrypt files/documents and demands the victim to use Bitcoins so the files/documents will be unencrypted (Pathak & Nanded, 2016).

3.3.6 Cyber-grooming

Owen, Noble, and Speed (2017) define grooming is someone who builds an emotional relationship with a child to gain trust aiming for exploitation or sexual abuse. Groomed victims are not limited to any age and can start in a short or long period of building the relationship, basically, for the purpose of exploitation, trafficking and sexually abuse (Owen, Noble, and Speed, 2017). The increase in the number of pornography and child grooming has become an international concern. Kierkegaard (2008) wrote an article based on the Internet Pornography Statistic Report authored by Ropelato (2006). The main concern is the involvement of underage children (under 18 years of age). About 4.2 million websites (i.e., 12 percent of total websites) are related to pornography. Ninety percent of children aged 8 to 16 are accessing pornography websites while doing their homework (Kierkegaard, 2008).

Al-Khateeb and Epiphaniou (2016) from the University of Bedfordshire have confirmed in their report National Society for Prevention of Cruelty to Children that 12 percent of children between the ages of 11 – 16 have received unwanted sexual messages. Kierkegaard (2008) emphasises that the freedom of using the internet increases the danger for the children to be involved in grooming, cyberbullying, pornography, and paedophilia. ICT development has aided sexual predators, stalkers, child pornographers, and child traffickers to exploit children. Kierkegaard also comments on the boundary of national legislation in cyberspace. Different nations get valid legislation within their boundaries, and it is more difficult to investigate cybercriminals from other nations due to this limitation. For example, “images which are illegal to view in the USA may not be illegal to view in Germany” (Kierkegaard, 2008) (p. 41).

A child-abuse convention to protect children against sexual abuse and sexual exploitation is an affirmative option. The formation of international conventions will assist with the protection of human rights, promote respect, and provide equal opportunities among each nation. The Budapest convention on cybercrime and

other conventions will be helpful to facilitate the cooperation power to work with other nations such as France, Europe, South Africa, Japan, the Philippines, and the United States. These countries will assist developing nations to harmonise cybercrime. According to Clough (2014), an international convention for cybercrime should focus on three main features of harmonisation: 1) comprehensive, 2) protection of rights and 3) representative.

3.3.7 Cyberterrorism

This section explores several definitions and thoughts from multiple authors to define the meaning of cyberterrorism. Different authors doubt the presence and reality of cyberterrorism, while others believe that cyberterrorist attacks already existed.

Gillespie (2015) combines the words cyberspace and terrorism to make clear definition of cyberterrorism. “It is a conjoining of cyberspace and terrorism to produce the notion of terrorism that takes place either in, or through, the internet” (p. 106). Ahmad and Yunos (2012) clarify that cyberterrorism was invented by Barrie Collin from California Institute of Security and Intelligence in the 1980s. Barrie Collin describes cyberterrorism as “the convergence of the virtual world and physical world form the vehicle of cyberterrorism” (p. 149).

Janczewski (2007) defines cyberterrorism as “politically motivated attacks by subnational groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets” (p. 14). Kenny (2015) also defines cyberterrorism as “computer generated attack that aims to gain information on other computers in cyberspace” (p. 121).

Iqbal (2003) defines cyberterrorism as “hacking with a body count” (p. 397). Gillespie (2015) argues about body count by giving an example on the financial attack. Attacking on the financial industry is considered to be terrorism (“subject to the motivation for the attack”) (p. 106). This type of attack affects the monetary strength and economic system but no bodily harm, no death or body count is involved.

Iqbal (2003) provides examples to clarify the activities of a cyberterrorist. A cyberterrorist can hack into a computer system and: break into an air-traffic system and change the computer programme to cause plane collisions; change the formula in pharmaceutical medical records to kill thousands of people; change the pressure in gas pipelines to cause explode; disrupt domestic banking system, international financial system, the stock exchange, and bank financial transactions.

Conway (2011) doubts about the existence of cyberterrorism and comments "that no act of cyberterrorism has ever yet occurred and is unlikely to occur at any time in the near future" (p. 26). Pollitt (2002) defines cyberterrorism as "the planned, politically driven attack against computer programs, computer systems, information and data, which results in violence against civilian targets by secret agents or sub-national groups" (p. 67). Bryan Foltz (2004) adds on that the cyberterrorism's threat exists, "even if no cyberterrorism has ever been committed" (p. 156).

After The United States attack on 11 September 2011, a report entitled "Cyberterrorism" was conducted by Symantec Corporation. In this report, Symantec Corporation (2003) states cyberterrorism is "increased in some popular culture but a solid definition of this word is hard to come by" (p. 1). The authors of this report also set a scenario to support the complexity of word cyberterrorism by pretending to ask ten people to describe the meaning of cyberterrorism. The authors confirm that at least nine different answers were given for this question. (This mean there is no agreed description to explain cyberterrorism) The report also suggests that the internet and computer technology had key roles in the execution of the September 11th terrorist attacks in The United States. This suggests that people need to consider "the big picture of the overall terrorist threat, rather than view one aspect in isolation" (Symantec Corporation, 2013) (p. 9).

Kenney (2015) further informs that the United States and other nations have come across multiple cyberattacks in recent years, but none have reached the level of cyberterrorism. Hardy and Williams (2014) give examples of cyberterrorist attack targets that wreak havoc and destruction. These targets are nuclear power systems, hospitals, air-traffic control systems, and stock markets (Hardy & Williams, 2014). Symantec Corporation (2013) and Denning (2001) provide similar observation

suggesting cyberterrorism attacks could lead to bodily injury, death, plane crashes, water contamination, explosions, and severe economic loss.

Based on information gathered above, the abovementioned authors have different interpretations, beliefs and meanings of the word cyberterrorism. Some authors believe cyberterrorism does not yet exist while others argue to the contrary. Akhgar, Staniforth, and Bosco (2014) query about the existence of cyberterrorism and then conclude that no clear performance of "cyber terrorism has occurred yet" (p. 16). They also give advice to people about the need to be aware of, and get ready for cyber terror acts in the future.

The authors of Symantec Corporation 2003 believe that the September 11th attacks are related to cyberterrorism as the internet and ICT technology were involved. A similar view provided by Seib and Janbek (2010) to show the methods of communication used by Al Qaeda, in relation to the 9/11 attack. A Hotmail account has been created by the cyberterrorists and members used the same username and password to access this email. "One person writes a message, but instead of sending it he saves it in the "draft" file and signs off" (p 26).

Al Qaeda's members from different places can access the message on the same Hotmail account, using the same username and password, and leave for other members to read and then delete. As the message remains in the draft and is never sent, no record retains in the ISP and no record traverses through the internet.

3.3.8 Insider Threat

Willison and Siponen (2009) warn organisations to be aware of external security threats and insider computer crime should not be underestimated. Identifying security threats for organisations is to involve both internal and external threats.

Greitzer et al. (2008) refer to insider threat as: harmful acts that trusted insiders might carry out; for example, something that causes harm to the organisation, or an unauthorized act that benefits the individual (p. 61).

Swartz (2007) informs about organisations, who concentrate on protecting their system from outside threats, often fail to secure them from the much larger threats created by internal employees. A report from Hanley et al. (2011) for the Software Engineering Institute (SEI), Hanscom, USA, summarises details on how, since the

establishment of SEI's CERT (Computer Emergency Response Team) in 2001, there have been 550 insider crime cases collected. "More than 80 of those crimes involved theft of an organisation's intellectual property by a malicious insider" (Hanley et al., 2011) (p. x1).

An expression of a scenario to display excerpts of possibilities of data leaks from insiders to outsiders when:

- An employee is unhappy at work. This employee has access to the company's sensitive information regularly and knows how the information is protected.
- An employee is disappointed with his boss when the employee recommends a close friend/family member to a higher position but then that position is entitled to someone else.
- An employee is planning to take a silent-resign due to dissatisfaction then the employee leaks the company's confidential information to other people.
- Most of the company's secret information is passed from the employee (insider) to friends or families who are not employed in the company.
- USB and laptop devices are lost and contributed to overall risks of data leakage to outsiders.

Willison and Siponen (2009) apply Situational Crime Prevention (SCP) techniques that could potentially be deployed as safeguard options to reduce insider risks. SCP is already practised in many of these, "controlling access to facilities (such as swipe cards for office access to increase the effort), extending guardianship (such as staff chaperoning of visitors to increase the risks), denying benefits (such as clear desk and computer screens for reducing rewards), and setting rules (such as information security policies to remove excuses)" (p. 135).

The preventative technique used for detecting burglary of electronic goods is different from the requirements for burglary of financial domiciliary or jewellery. Examples of SPC tools are the installation of surveillance equipment in the vandalism areas, the installation of security screens for road traffics, for drug markets, and for banks which are very effective in detecting criminals.

3.3.9 Push Payment Scams (PPS)

Push Payment (PP) is a method used by banks or other Payment Service Providers (PSP) to transfer money from customer's account to another account as payment for goods or services. The customer must provide the consent first, to authorise the bank and PSP to pass this transaction and make the payment. This authorisation process is known as Push Payment (PP) in which the customer trusts the PSP to deal with their money for payment of good or service. The PP system is noted to be the major issue in some places. In the UK, PP scams are the second biggest cause of fraud payments. According to Tankard (2018), about 19,000 people in the UK were involved in PP scams between January - June 2017, claiming a total loss of £100m.

Two common attack methods are actively organised by the scammers to defraud customers. These are email hijacking and Wi-Fi eavesdropping. A man-in-the-middle attack is a form of email hijacking. As the customer is ready to transfer money, the scammer tries to intercept the communication between the PSP and the customer. The scammer setups an illegitimate email to mislead both PSP and customer to deposit the money into a different bank account number. Both PSP and customer have failed if money is deposited to the scammer's bank account.

Wi-Fi eavesdropping is Wi-Fi Pineapple which is a handy Wi-Fi node and a "custom WLAN (wireless local area network) router designed by Hack5" (Kropeit, 2015) (p. 11) that the scammer uses to install a free Wi-Fi hotspot and place it with a legitimate name in public areas such as café, waiting rooms, hotels, hospitals and airports. All these areas are completely open to the public. To access this free Wi-Fi hotspot, the user must provide personal information such as name, password, address, email or ZIP code. Public Wi-Fi networks are unsafe and have no protection for internet users according to (Consolvo S et al., 2010).

At any point where a scammer reaches a stage of performing as a gate-keeper to the internet, the scammer will get more opportunities to perform man-in-the-middle attacks. For example, a scammer enables to perform SSL-attacks (SSL stands for Secure Sockets Layer) by directing the internet user to access an unencrypted website or a bogus website. The scammer's primary target is to exploit the victim

who is connected to the free Wi-Fi hotspot to gain bank confidential information such as username and login details (Tankard, 2018).

3.3.10 Home-based internet users (HBIU)

Kritzinger and von Solms (2010) emphasis the importance for all Internet-users to understand the dangers of using the internet, the importance of keeping personal information secured, the risks of not following security procedures and the consequences of losing personal information in the wide area of cyberspace. The authors also highlight some of the vulnerabilities of Home-Based Internet Users (HBIU) as HBIU are not aware of the internet's risks and have limited knowledge of ICT security procedures.

Anderson and Agarwal (2010) agree with the security vulnerability of HBIU as these people are individual and home-based users. No supports or no other people to ask questions when they get stuck in difficult situations. Compared to workplaces where the environment is protected by surrounded technical staff specialised in securing hardware and software. They are not entitled to training support. The authors have concluded the results of their study that HBIU's "intention is formed by a combination of social, cognitive and psychological components" (p. 637).

A similar view is held by Furnell, Tsaganidi, and Phippen (2008) about the security vulnerability where the major challenges faced by HBIU are lack of knowledge or inclination to take steps to protect themselves. HBIU is "now accounts for as much as 95% of targeted attacks" (p. 235). Kritzinger and von Solms (2010) contrasts HBIU and Non-Home-based Internet Users (NHBIU) saying that's HBIU are not observed under-a-watchful-eye and no compulsory enforcement is undertaken. They are dependent on their own IT security knowledge and follow no guidelines, policies, or regular security training enforcements. HBIUs are not forced to attend appropriate IT security training and are becoming more vulnerable to security threats.

NHBIU refers to users that access the Internet from industrial areas, academic, business, education, organisations, and government ministries. Most NHBIUs are more secure as they are exposed to more compulsory security policies, guidelines, training, awareness courses, and other compulsory security preparedness. NHBIU are regularly observed under-a-watchful-eye by their workplace to ensure they are

competent with IT security knowledge and follow the IT security regulations and rules (Kritzinger & von Solms, 2010).

3.4 Cybersecurity Defences

3.4.1 Phishing Prevention

Phishing has been identified as a major concern, and the United States is the first nation to enact laws to fight against phishing. The Federal Trade Commission (FTC) added phishing to their cybercrime list in January 2004. George W. Bush, the former President of the United States agreed to establish a task force in May 2006, to ensure effective prevention and to identify people who plan to attempt cybercrime (Mohammad et al. (2015).

From Machine Learning (ML), approaches have used several tools to filter many emails and then separated classified phishing emails as spams. According to (Lalitha & Udutha, 2013), Mozilla Firefox web browser uses ML tools to check the phishing site by downloading a blacklist to a local machine to identify phishing. From the results, "35 new phishing sites have been detected per hour" (p. 1734). Another prevention technique emphasises by Florêncio and Herley (2007) is about the using the of One-Time-Password (OTP) system to limit the phishers' ability to "exploit any information obtained" (p. 27). OTP is a password which is valid and used for only one login session to access a digital or computer system. The main advantage of OTP is a second user or a prospective intruder or a scammer is unable to use the same login password to access into the same transaction. OTP is only set up to use once and never again.

Additionally, some automated detection tools are used by Internet Service Providers (ISP), websites, mail servers and clients to detect and block phishing messages and phishing websites. An automated email tool commonly uses a machine-learning algorithm, spam filtering and statistical classifier techniques to detect potential phishing messages. For example, the Netcraft automated tool provides multiple internet security services, including anti-phishing and anti-fraud services, Payment Card Industry (PCI) scamming and application testing. Netcraft combines blacklist and heuristic techniques. Heuristic uses the SpoofGuard tool for checking URLs and hostnames for possible web spoofing or phishing. Blacklist uses Cloudmark to identify and produce a list of phishing URLs (Zhang, Hong, & Cranor, 2007).

Also, to send an email-message to a mailbox, the Cloudmark tool scans the entire email (header, body, subject-line, and footer) and creates a new fingerprint of the content, image, URL, and code. The next phase is to compare and look for similarities of both fingerprints, and the existing and new fingerprint from the Cloudmark database. Similarities of both fingerprints to message are classified to be not-spam or spam based on similarities to another message in the database. All email-messages sent to Cloudmark mailboxes are fingerprinted and not all fingerprints are spams (Return Path, 2019).

3.4.2 Cyber Resilience

Resilience is the ability to recover quickly from a tough and difficult situation. In the concept of cybersecurity, Björck, Henkel, Stirna, and Zdravkovic (2015) define cyber resilience as the "ability to continuously deliver the intended outcome despite adverse cyber events" (p. 2). Conklin, Shoemaker, and Kohnke (2017) agree; cyber resilience is to ensure the ongoing process of the ICT core-operation and functionalities or fast recovery from cyber events). Conklin et al. (2017) come with a similar point of preventing the cyber attacker from harming the most critical assets of an organisation and to avoid access beyond the basic restricted security control countermeasures.

Also, Conklin et al. (2017) contrast cybersecurity and cyber resilience. They stated that cybersecurity concentrates on access control to ensure comprehensive securities that are in place to protect from unauthorised access either internal or external sources. Cybersecurity also targets all point of entries into the computer systems to detect all types of unauthorized access. Cyber resilience targets security architects to ensure the effective core functions of the organisations' systems are operated and non-stopped. Cyber resilience ensures the practical functionalities of organisations are uninterrupted or ensure continuous improvement and "ability to recover within an acceptable period" (p. 106).

Based on the concept of quick recovery, no matter how large/small of the impacts were involved, the mindset of victims is to return to a state of control and return to normal operations.

3.5 Cybercrime in developing Nations

3.5.1 ICT development in the South Pacific Islands (SPI)

Wallsten (2005) concerns over the slow growth of the internet in poor nations. People in wealthier nations have better opportunities to benefit from ICT development than in poorer nations. Wallsten stated that "developing countries require donations of facilities and training in order to spark faster internet growth" (p. 501). The limitation of accessing the internet is inversely proportional to financial power; the wealthy nations get more power to access and facilitate the growth of ICT.

The fast growth of mobile technology with 4G standard has great influences for the people of the Pacific. In 2008, the penetration rate for six islands (Tuvalu, Kiribati, Solomon Islands, Papua New Guinea) was less than 16 percent (Cave, 2012) (Finau, Samuwai, & Prasad, 2013). Cave (2012) summarises the ICT growth in Samoa, Vanuatu, New Caledonia and Fiji as to have been increased in their penetration rate to more than 80 percent. The mobile penetration rate in Tonga has increased from three percent in 2002 to 53 percent in 2011. Papua New Guinea's mobile penetration rate has increased by 32 percent, from two percent to 34 percent from 2006 to 2011. The same report shows that 53 percent of the people of Papua New Guinea use the mobile phone to listen to the radio stations.

While ICT development provides significant benefits, it also provides significant opportunities for criminal activities. Kshetri (2013) notes that high-speed broadband, social media, cloud computing, and mobile phones have spawned the economic, social, and political growth in developing islands in the Pacific. These are influential effects but also become the target points for all kinds of cybercrimes (Kshetri, 2013). Finau et al. (2013) show a similar view about the revolution of ICT development in the Pacific that has both provide significant opportunities and significant risks.

Mow (2014) highlights some of the ICT challenges encountered with SPI. In the Solomon Islands, ICT challenges are involved with the formation of a national ICT policy and low update in certain groups in rural communities and general improvement issues in sustainable, wellbeing, environmental awareness, resource management and conflict resolution. In Fiji, one of the major issues encompassing

their e-government development at the standard-level, is antagonism towards United Nations e-government benchmarks.

Shortage of cybersecurity experts is a nationwide issue. Cybersecurity specialists focus on the overall safety of the networks, software, and data centres. Coventry and Branley (2018) raise major cybersecurity issues in the health industry such as shortage of money to upgrade software and lack of cybersecurity experts is aggravated. Laulaupea'alu and Keegan (2019) confirm that “Tonga is in need of specialised security experts” (p. 190). Ideally, if the shortage of cybersecurity is a worldwide issue and Tonga is incontrovertibly needing cyber-experts, undoubtedly, SPI certainly requires more cyber-experts for the overall safety and needs to upgrade the system to meet international ICT standards.

3.5.2 National Cybersecurity Strategy (NCS), ISP and ICT Framework

Goodwin and Nicholas (2013) define National Cybersecurity Strategy (NCS) as the vision that articulates priorities, approaches and principles to understand and manage risks at a nationwide level. NCS is varied in different nations where in some countries they emphasise intellectual property, in other nations they focus on serious infrastructure risks, while in other states they focus on developing cybersecurity awareness based on newly connected citizens. A well-developed NCS facilitates the needs of the private sector, government and the country’s citizens. Goodwin and Nicholas (2013) further extend that NCS assists with:

- Educating citizens about the characteristic of the problem and providing appropriate approaches;
- The opportunity for organisations and citizens to offer inputs into a public dialogue;
- Articulating the national priorities, policies, principles and programmes (4 ps);
- Stipulating the missions and roles of NGOs and government agencies;
- Specifying goals, metrics and milestones to measure progress in addressing issues;
- Providing appropriate resources (p. 4).

According to Laulaupea'alu and Keegan (2019), the purpose of Information Security Policy (ISP) is to “ensure that IT users comply with guidelines and rules to safeguard information stored within organisations, to regulate employees

security performances, and to prevent violation of information security systems" (p. 190).

ISP is defined by Bulgurcu, Cavusoglu and Benbasat (2010) as a statement of the responsibilities and roles of an employee to protect the ICT resources and information of an organisation. ISPs establish rules involved with security issues in the organisation and provide instructions to be followed by the employees.

Safa, Von Solms, and Furnell (2016) clarify the technical provisions of authentication, anti-virus, anti-phishing, anti-malware, anti-spyware, anti-spam, firewall and Intrusion Detection Systems (IDS) are not guaranteed to secure the information. Cybercriminals target individuals rather than computers to create breaches. The characters of inappropriate ISP that lead to breaches are the; "use of social security number as password and username, write the password on a piece of paper, share password and username with colleagues, open an unknown email, download an attachment, and download software from the Internet. Safa et al., (2016) conclude that acceptable ISP should combine with technical features. Combination of multiple cybersecurity approaches mitigates the risk of security breaches (p. 70).

Developing countries are required to develop and implement proactive strategies and procedures to meet the national level of cybersecurity strategy and framework. According to Dennis, Jones, Kildare, and Barclay (2014), a study conducted by the UN in 2013, "revealed that a significant number of countries are without a national cybercrime strategy" (p. 1). Nations in the Caribbean, including Jamaica, are still without NCS and security framework. Dennis et al., (2014) suggest a National Cybersecurity Framework (NCF) for Jamaica to focus on CIA triads (Confidentiality, Integrity, and Availability) and to serve as a design plan for both public and private sectors in Jamaica. Also, the framework is to be based on standards and best practices from the "ISO 27032, COBIT 4.1, ENISA and ITU to provide the necessary robustness in the baseline procedures" (p. 8).

Dennis et al. (2014) also stated that developing countries do not have the necessary expertise and resources to control cybercrimes. The developing nations, such as Jamaica, cybercrime is a national and global issue and cybercrime is high on the national agenda. Furthermore, developing countries need to prioritise cybersecurity

awareness and make recommendations to implement NCFs for the Caribbean, Jamaica and other developing nations. Jamaica is considered by FAO (2021) (paragraph 6) as one of the "slowest growing developing countries in the world". Tonga as a developing nation is in a similar situation. Laulaupea'alu and Keegan (2019) state that 51 percent of government organisations in Tonga deploy their own Information Security Policy (ISP). The authors recommend that the Government of Tonga should provide ISP to encourage users to comply with the rules and guidelines and to "secure information stored within organisations" (p. 190).

White House (2018) released the National Cyber Strategy of the United States of America, signed by Donald J. Trump, the President of the U.S.A. in September 2018. President Trump's top priority is to ensure the security of the people of America and to be safe from the involvement of cyberspace. The president has also mentioned that America invented the Internet and distributed to the world and America must be ensured to secure it for future generations.

The announcement of NCS demonstrates the full commitment of President Trump to enforce cybersecurity abilities to secure America from cyber-threats. White House (2018) summarises four main focuses of the United States' NCS:

- 1) Defend America by protecting the data, functions, networks, and systems;
- 2) Promote prosperity by encouraging digital economy and strong national innovation;
- 3) Maintain peace and security; to discourage and put punishment for people who initiate cyber-tools for malicious activities. The United States is to strengthen the cybersecurity capabilities by making partnerships and allies; and
- 4) Expand American's cybersecurity influence abroad and to be reliable, interoperable and secured.

NCS is a crucial element of ICT preventions and awareness and the CIA (confidentiality, integrity, and availability) of data/information. The United Kingdom has invested £1.9bn on NCS strategy (2011 – 2016) for the nation's cyber workforce to protect online citizens and businesses from cyberattacks (Pultarova, 2016). The two well-known nations, the UK and the United States, have set examples to the world about the importance of NCS and the concern about the safety of the world from evildoers and cyber attackers. These two nations lead the

combat on cybercrimes nationwide through prioritising NCS and security frameworks at the top of cybersecurity agenda.

3.5.3 Lack of Cybersecurity-law experts

Tropina (2016) raises the issues of the gap between law officials and criminals. The author stated that the enforcement of the law is hamstrung because of the technical gap between law enforcement officials and sophisticated criminals. Tropina believes that the law officials are much less equipped with technology while sophisticated criminals are always looking for ways to cheat technology. A similar view from Broadhurst (2006) about law enforcement officials and agencies where Tropina stated that in many jurisdictions, law enforcement agencies are "unable to respond effectively to cyber-crime and even in the most advanced nations" (p. 410). Dennis et al., (2014) agree that ICT development for developing nations is ineffectively managed cybercrime due to necessary resources and expertise by stating that it could be helpful "to assess the requirements of existing national regional and international instruments and to assist countries in establishing a sound legal foundation" (p. 2).

Mohammed, Mohammed, and Solanke (2019) provide a similar view that the slow process in cybercrime investigations was caused by insufficient cybersecurity knowledge and a skill gap of law enforcement. Understanding of applications and underlying technology are required by judges to act on judging cybercriminal cases and civil courts (Mohammed et al., 2019). Kundi, Nawaz, Akhtar, and MPhil Student (2014) agree that the lack of cooperation with international law does little to ease the danger around the globe in cyberspace. The authors also mention that there is no proper legislation established to prevent the cybercrimes/electronic and to protect the users from e-Frauds.

A direct recommendation made by Laulaupea'alu and Keegan (2019) to the Government of Tonga about the need for cybersecurity experts to look after the IT systems of Tonga. Laulaupea'alu and Keegan clarified the need for Tongans to partake in cybersecurity training overseas as education will empower high-quality understanding and bring advanced knowledge of cybersecurity responsibilities. They also informed the government that the total costs involved with the overseas

study is small compared to potential cost and damage that may be involved in the future.

3.5.4 Cyber-deception in Ghana

Danquah and Longe (2011) refer to cyber deception as the involvement of ICT for stealing and ruse purposes. Examples provided by the authors include credit-card fraud, intellectual property and privacy violence. Cyber deception and theft have appeared in different forms such as identity theft, pagejacking or spoofing, auction fraud, credit-card scheme, advance-fee fraud or fraud mail or 419 mails and phishing.

Danquah and Longe (2011) conducted an ethnographic study in Ghana to collect information from victims about the methods used for cyber deception. The research findings conclude that pagejacking, spoofing and merchandise/auction frauds had little involvement in Ghana. The authors made recommendations to devote more attention to the following areas such as: Key Loggers, VIP Sections and Black Magic Factor. Further recommendations emphasised the deployment of policy, practices and law, including a law to mandate all the Internet Cafés to obey cybersecurity standards organised by National Standards Boards (NSB).

Boateng, Longe, Mbarika, Avevor, and Isabalija (2010) state that most cybercrimes in Ghana are initiated by Internet Cafés and are related to child pornography, downloading films and hacking websites to access to credit cards. Danquah and Longe (2011) make recommendations for a proper law to assist investigators in searching for electronic evidence relating to cybercriminal activities conducted by the Internet Cafés. At the same time, the law enforcement agencies must ensure their cybercrime investigators are equipped with the right resources for complex investigation. Finally, the recommendations include enforcement of Information Security Policy (ISP) for public organisations and to emphasise information security practices in the modern day school curriculum.

Social engineering has become a prominent feature in theft and cyber deception in Ghana. Danquah & Longe (2011) discussed a case of a women, Anita, an Australian High School teacher who has been involved in sending money to a person in Ghana, is an example of social engineering deception. Both the victim, Anita, and the fraudster, have connected through the online dating website. More than $24,745 has

been paid by Anita to the scammer with the expectation to pay back the money upon the fraudster's arrival to Australia. The scammer is believed to be a Canadian archaeologist living in London, who worked in Ghana and this case is claimed that there is a connection of the scammer with a chief in Ghana.

3.5.5 Online Banking (OB) in Nigeria

A. E. Ezeoha (2006) discusses the challenges of Online Banking (OB) and the rapid growth of mixed development in Nigeria. Mixed development referred to in this scenario are developments in Africa such as rapid ICT growth, the fastest growing ICT market, low international-call tariff, fastest-growing telecom-market, lowest-costs in Sim packages, political and economic corruptions, English speaking states, and the rapid development in OB services. With the rapid growth of mixed development, Nigeria needs regulatory cover to meet global ICT growth and to update regulations for financial institutions and banks to meet international standards. Ezeoha (1970) mentions that a nation like Nigeria where fraudulent acts are rampant, regulating the OB becomes a nationwide concern and global attentions. The capacity of the current regulation is complex as national banking laws were designed and formulated before the advent of Internet (Ezeoha, 1970) (paragraph 4). Yoon (2010) raises some important factors about OB such as ease of use, transaction speed, information content, design and security. Security is an important aspect as OB as it is internet-based service and open network. Although various cybersecurity techniques are applied such as digital certificates and signatures, cryptography and authentication, customers are still worried about the security of monetary transactions when using the Internet (p. 1299).

Oni and Ayo (2010) confirm that Nigeria is the fastest growing telecommunication state in Africa and OB services have been actively involved in ICT development. Electronic payments have been recorded and there were 360 billion bank transactions verified in 2008 and the Automated Teller Machine (ATM) remains the most widely used bank services. Customers inform that e-banking (or OB) is more convenient, easy-to-use and useful but there is a major concern with the reliability of the system. Security measures and data privacy of OB are the major subjects that bother the minds of both the intending and existing users. Oni and Ayo (2010) conclude about e-Banking in Nigeria that there is a mistrust in the

integrity of the security of e-banking technology and the capability of e-Banking systems to protect privacy.

3.6 Cybersecurity in the SPI

3.6.1 Cybercrimes in Fiji

Nisha and Farik (2015) discuss a cyber deception case in Fiji in August 2016. It started when several fake profiles displayed on Facebook, pretended to originate from the Reserve Bank of Fiji (RBF), promoting fake investments, lotteries and loans. RBF identified this scam when an innocent user approached and sought formal approval from RBF to deposit/send money to scammer's fake account. In response, RBF, Financial Intelligence Unit (FIU) and Fiji Cybercrimes Unit took immediate action and closed this fake account. Three victims were caught in this fake activity as these victims already deposited money to this fake account and this scam is believed by the investigators to have originated in Africa.

In 2016, Fiji ANZ Pacific officials revealed that ATM and credit card scams have become predominant in Fiji costing the banking industry millions in losses. Nisha and Frank (2015), outline some ATM scams that have happened in Fiji. Two customers noted that credit accounts were scammed/withdrew $2,000 in Ukraine and $10,000 in Saudi Arabia. In response, the ANZ closed down these accounts and referred to FIU for further investigation. Also, a taxi driver informed Fiji Police about a group in Lautoka (the second largest village in Fiji) for suspicious withdraws of money from ATMs. Six Chinese were arrested with 384 Westpac, ANZ, and BSP ATM false cards and over FJ$22,807 in cash. Another social media harassment attack which is uncommon to happen in Fiji was stated by Nisha and Farik (2015) as an 8-year-old student from Suva got raped by a 17-year-old boy from Nadi. The source of communication between these two was Facebook, where they arranged and agreed to meet in Nadi.

3.6.2 Online scamming in Fiji

Pandey, Shah, Sharma, and Farik (2016) report on the number of cybercrimes undertaken in Fiji from 2013 to 2015. A total of Fiji $305,000 (see *Table 9*) has been lost from several companies in Fiji for ordering materials from overseas but the money was illegally diverted to other destinations. Companies have ordered

their goods with the expectation to receive these items, but the payments diverted to different destinations and no goods were delivered to the respective companies.

Table 9: Illegal Money Transfer in Fiji

Time	**Description of Criminal**	**Amount Loss ($)**
2013	In Suva, a company passed a single overseas transaction, a payment for purchasing goods from Taiwan. The payment was illegitimately diverted to different destinations, via the United Arab Emirates (UAE) and finally to India.	US$65,000
2013	In Suva again, three online transactions for payment of raw materials ordered from Belgium and China. The payments were illegitimately diverted to UK.	US$44,000
2014	In Savusavu, a single overseas transaction for payment of an excavator from New Zealand. The payment was illegitimately diverted to Scotland.	NZ$58,000
2014	In Suva, an agency ordered clothes from Israel and the payment was illegitimately diverted to the UK.	US$101,000
2014	In Suva, a single online transaction for payment of spare parts from China. The payment was illegitimately diverted to a different company in China	US$10,000
2015	In Nausori, a company's payment was illegitimately diverted to the UK, purposely for the supply of supermarket food from Pakistan.	US$13,000
2015	In Suva, a company ordered spare parts from China, payment was illegitimately diverted to a different company in China.	US$14,000
	Total Loss	**US$305,000**

Pandey et al. (2016) take another summary report of 18 cases to relate to cyber-laundering through email-spoofing from 2013 to 2015 (see *Table 10*). This investigation has been investigated by Fijian Intelligence Unit (FIU) and the report is summarised in the following table.

Table 10: Cyber-laundering money in Fiji

Numbers of Cyber-laundering offences	**Amount (Fiji (F$))**
Four (4) attempted cases	$300,000
One case (1) recovery of stolen fund	$60,000
Thirteen (13) cases of stolen funds	$724,000
Total eighteen (18) attempted cases	**$1,084,000**

Tamanikaiwaimaro (2010) examines cybercriminals in Fiji and reports that all levels are affected including national governments, private and public sector, and individual citizens. The author also states that cybersecurity is a new phenomenon with policies and national strategies yet to be addressed. And, the vulnerabilities of the computer systems are due to poor laws, lack of applicable policies and lack of security framework. Tamanikaiwaimaro also mentions that the Pacific Islands are vulnerable to common cyber-attacks happening around the world. These cyber attacks are classified as phishing, malicious software, brute force attacks (SSH secure shell) and telephone hijacking. Tamanikaiwaimaro gives an example of a telephone hijacking case that happened in the Cook Islands in 2007. There are no details of this case but the author states there was a disruption in the PSTN (Public Switch Telephone Network) resulting in the loss of over "US$100,000 in just four hours" (p. 1). Similarly, in the Marshall Islands, a severe Denial of Service (DOS) attack had disrupted the island's services for two days (p. 2).

Tamanikaiwaimaro (2010) recommends for the stakeholders in Fiji to take action to: conduct more workshops to identify security weaknesses and develop strategic plans that can be used nationwide; to form a working group to identify cybercrime; research on cybersecurity in Fiji; look for potential local, regional and national partners; to develop ICT policy and national strategy.

These recommendations are intended for Fiji's cybersecurity awareness but they are well-matched to other Pacific islands including Tonga. The scams discussed by Pandey (2016) suggest online scamming is becoming prevalent in other Pacific Nations too. Similar cybercrime cases have been discovered in Tonga in 2016 such as email phishing, data theft and data los", ransomware, and unauthorised access discusses by Laulaupea'alu and Keegan (2019) (p. 188).

3.6.3 Cybersecurity Law in the SPI

Kundi et al. (2014) bring the idea that cybercrime can be controlled and regulated through cyber legislation. The infiltration of cybercrimes is due to inadequate technology, resistance to cooperate with international law and the absence of legislation. The authors conducted research in Pakistan to assess the challenges involved with the prevention of cybercrimes. The authors conclude that many studies report confirm that computer users "do not know about the cyber laws" (p. 68). This is the reason why they become victims of e-crimes and e-frauds in the developing nations "generally, and Pakistan specifically" (p. 68). Kundi et al., (2014) asks Pakistan legislators to pass two-tier-model legislation that can be able to withstand the complexities of cyber-world.

Saini, Rao, and Panda (2012) give examples of countries in Africa such as Nigeria, Tanzania, Tunisia, and Kenya who are "almost-free from policies and cybersecurity-laws" (p. 204). They emphasise three categories to assist in trying to overcome cybercrimes. These are education, cybersecurity-laws and making policy. These three categories are valid to African nations and could also apply to the South Pacific nations. Kshetri (2013) states that Development Pacific Island Economies (DPIEs) have fallen behind in the process of passing cybersecurity-laws which makes it more difficult to deal with offenders.

Law enforcement in Fiji is inappropriately functional. A clear case has been carried out in Fiji that reflects the weakness in enforcing cybercrime law. This is where an accuser has cheated victims by advertising items to be purchased online. Payments have been paid by victims to the accuser, but the items have not been delivered. The judge has pre-informed the accuser that charges may drop if money is refunded to the victims before the hearing date. As a result of the judge's mercy, the same accuser reappears in court for acting the same cybercriminal cases with the huge amount of money lost from new victims. (Pandey, Shah, Sharma, and Farik (2016) conclude that "Fiji should incorporate more specific and stringent laws against computer offences to better cater for the novel and innovative" (p. 219).

3.7 COVID-19 Scams

COVID-19, a Severe Acute Respiratory Syndrome (SARS) coronavirus 2 (SARS-CoV-2), is akin to SARS-CoV which triggered SARS to thousands of individuals

in 2003. Yi, Lagniton, Ye, Li, and Xu (2020) stated that SARS-CoV-2 might be initially transmitted from bats and spread through the same process of SARS-CoV. COVID-19 then has greater brutality and mortality impact than SARS-CoV, which causes major effects on men than women and more elderly rather than youth. According to Lu and Shi (2020), in December 2019, patients were noted to have signs of fever, dry cough and a decrease in white blood cells and still classified as Fever of Unknown Origin with pneumonia. The number of patients has continuously increased in Wuhan where it was initially started. Therefore, COVID-19 is noted to spread through human-to-human transmission, transmitted to other nations and seriously imperilling human life, the World Health Organisation announced that COVID-19 is to be noted as a "Public Health Emergency of International Concern on 30 January 2020" (Lu & Shi, 2020) (p. 564).

While the world top agenda is focused on COVID-19 with the global fast killing rate and to explore a vaccine for this pandemic virus since the end of 2019, fraudulent actors use as opportunities of this worldwide health crisis to defeat other individuals to gain benefits. Cyber-actors have normally headlined the coronavirus to send scams to defeat victims. "Malicious actors are also using COVID-19 or coronavirus-related names in the titles of malicious files to try to trick users into opening them" (Amad, 2020) (p. 2). According to Analytica (2020), the UK National Fraud Intelligence Bureau estimates the cost of over than 800,000 pounds in the UK in February 2020 which was all related to COVID-19 frauds.

The COVID-19 pandemic has changed the normal physical attendance to the worksite to being the world's highest number of employees bound to work from home remotely. Ahmad (2020) warns about the consequences of working from home which required people to be aware and to gain knowledge of phishing scams, the fastest growing type of cybercrime. The author stated that cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. Working from home should make organisations aware of providing immediate training about cyber-privacy and cybersecurity failings. Ahmad also stated that failure to gain appropriate cybersecurity knowledge, the "cybercrime damage may costs as much as double by the end of this year" (p.1).

In April 2020, the United States Attorney and the Internal Revenue Service (IRS) Criminal Investigation warned that the upcoming payments of taxpayers was an opportunity for fraudulent acts from cyber actors. To avoid being scammed, the IRS advises taxpayers to 1) hang-up the phone if someone asks for payment details as the IRS does not, and will not, use or ask on the phone to verify details; 2) Not click on any links if any text or email was sent from IRS emphasises a way to get money faster; 3) taxpayers payment is going to be directly deposited to bank account previously mentioned on tax return form; 4) If someone knows a call is from a scammer, do not tell the scammer that the contact is a scam and you want to beat him, just hang up the phone (Department of Justice, 2020).

Okereafor and Adebola (2020) were aware of the Confidentiality, Integrity, and Availability (CIA) of global internet users. The authors stated that Coronavirus or COVID-19 is likely "one of the most searched words on the internet today" (p. 3). As web search engines are busy on searching keywords string like COVID-19, coronavirus, china, virus, Wuhan disease and other related strings, an opportunity for scammers to spread malicious codes while the focus is on coronavirus disease. Furthermore, majority of coronavirus gimmicks offer health updates and relevant information about the international health emergency. Emotet, a well-known coronavirus-related malware, is a Trojan horse malware programme targeted to obtain financial credentials from victims by inserting a calamitous code into the computer-infected programme (e.g., Microsoft Word document) to gain sensitive information.

Okereafor and Adebola (2020) make recommendations to maintain safety from coronavirus scams. These are to test commercial websites before making payments; keep clear of clicking doubtful attachments; keep clear of clicking on doubtful URLs and web addresses; keep an operational back-up of data; verify the source of information; fine-tune digital readiness (p5 - 8).

Okereafor and Adebola conclude that every literature on coronavirus appears on the internet as attractive features that increase the tendency for the users to download adware, ransomware, spyware and other malicious software. The anxiety and panic related to COVID-19 increase the chances for cybercriminals to take advantage of the human fear to attack victims by using coronavirus information.

3.8 Comments

After this review, the cybercrimes and cyberattacks were originally started from wealthy nations (such as China, UK, The United States and so on). These impacts were transmitted from these nations and are now affected Australia, New Zealand, Fiji and other South Pacific Islands including Tonga. Laulaupeaʻalu and Keegan (2019) discovered new cybersecurity issues that occurred in Tonga. In the Introduction chapter there is a section known as Cybersecurity in Tonga. This section is a part of the literature review and the main reason for placing in the front of this thesis is to prove there are cybersecurity issues in Tonga that are required to take further investigation and to find the root causes of these issues. Therefore, it is worth conducting this research project based on evidence that Tonga's ICT system is vulnerable to cybercrimes and cyberattacks.

As mentioned previously, the major challenge of this research project is COVID-19. Due to the unavailability to meet face-to-face interviews with the survey participants, there are some major sections in the literature review that were unable to implement during the data collection phase. It was up to a stage that the researcher, Siuta, decides to remove some of these sections from the literature as there were no actions or investigations on these issues during the data collection. However, the researcher decided to keep this information as it will be valuable for future research. Some of the areas that are not covered in this research are: Cyber Resilience, Push Payment Scams (PPS), Insider Threat, Cyberterrorism, Cybersecurity Law in the South Pacific Island and COVID-19.

[FYI: A Journal Article, called 'COVID-19 muddles talanoa and vā: Perceived connections and uncertainties', was recently published by Waikato Journal of Education authored by Laulaupeaʻalu S. (2021). Again, another Journal Article, called 'Cybersecurity Law in the South Pacific Island', authored by Siuta Laulaupeaʻalu will be published soon. These two journals are starting the investigation process about missing sections that were unable to implement in the data collection phase].

CHAPTER FOUR

4. METHODOLOGY

4.1 e-fanongonongo tokoto (e-ft)

The author of this thesis deployed ***e-fanongonongo tokoto*** (e-ft) as a methodology to communicate and collect data while being restricted by COVID-19 lockdowns and travel bans. This methodology is based on indigenous ways of communication in Tonga called *fonongonongo tokoto*. The deployment of e-ft was utilised to connect from New Zealand to the survey participants in Tonga. The COVID-19 pandemic became the major interruption factor to this research project. The original plan to travel to Tonga to conduct a face-to-face interview with the survey participants was cancelled and e-ft was adopted to solve the issue of data collection.

In this context, 'e' stands for electronic. A lowercase 'e' is added to the word mail to form a verb – electronic email or e-mail or email. A similar procedure takes place in this method as lowercase 'e' is added in front of the two different Tongan words *fanongonongo* and *tokoto*. Both words are verbs or action words.

The word *fanongonongo tokoto* is discussed in Section 2.2. In this section, additional information is added to clarify these two words (*fanongonongo* and *tokoto*) to match the meanings with the methods applied to contact and collect data from Tonga. Churchward (1959) defines *fanongonongo* and *tokoto* separately and then combines them to form one meaning. *Fanongonongo* is "to make publicly known, to publish, promulgate, proclaim" (p. 140) and *tokoto* is "to lie (down)". There is another way of communication called *talanoa* (conversation/discussion) which is known as *talanoa tokoto* or "to talk while lying down" (p. 490). *Talanoa tokoto* and *fanongonongo tokoto* were both applied in communication with the survey participants in Tonga.

Again, Churchward (1959) combines the two words to form *fanongonongo tokoto*, which means "to publish lying down, to publish or announce by telling to one's nearest neighbour," (p. 140). Latu (2017) defines a similar meaning as the passing of "words from one person to another, *kainga* to *kainga*, or generation to

generation" (p. 127). *Kainga* means "relation, relative; brother or sister in the sense of comrade or compatriot" as according to Churchward (1959) (p. 244).

There is no exact time when the *fanongonongo tokoto* started but there was a story in Tongan history, the offering of 'Iloheva, a loyal lady from another clan to the ancient *Tu'i-Tonga* (King of Tonga) for a progeny-produce offspring. The *fanongonongo tokoto* was the communication method used to converse between 'Iloheva and the king. Based on this information, the cohabitation story of bringing 'Iloheva to become pregnant to the *Tu'i-Tonga*, the methodology of using *fanongonongo tokoto* was invented before 950AD (Latu, 2017) (p. 161).

4.1.1 Contextualising e-fanongonongo tokoto

Fanongonongo tokoto as an ancient way of communication is where a message is passed from one *fale* (house) to the next *fale* by way of *tokoto* (lie down). A person lies-down in *lotofale* (lounge) and *kaila* (shout) or *talanoa tokoto* to the *kaunga'api* (neighbour) to convey the message initially delivered from the first *fale*. The message is delivered in the same way until it reaches the last *fale*. The *fanongonongo tokoto* was utilised and still put into practice in Tonga through direct communication or *kaila* or *talanoa tokoto* from *fale* to *fale* or face-to-face conversation until the message reached the last *fale* at the end of the village.

Pre-contacts were made by the author from home residence in Hamilton or UoW to introduce to the participants the purpose of the research. Tongan citizens responded and offered to assist by returning emails and Facebook responses. One of the responses was from the Prime Minister's Office to offer contact emails of senior officials to other government ministries. Other people offered to act as contact points where the questionnaires were sent to them and then they delivered the questionnaires to each participant via emails or physical copies. In this way, the questionnaires were able to be distributed to many regions of Tonga.

The way of sitting in a room at home or in the room at the UoW to perform the communication and sending of the questionnaires to Tonga is like the traditional *fanongonongo tokoto* performed by Tongans in ancient times. Instead of *kaila* (shout) or *tala* (convey) to the next *fale* (house) to deliver the message, the message is delivered through electronic devices. The form of e-ft to communicate

with the participants in Tonga are e-mail, Zoom, Facebook and Facebook Messenger.

Instead of continuous practicing of local *fanongonongo tokoto* within the Tongan community, the deployment of e-ft extends the way of communication not only within the local Tongan community but to communicate with the outside world. The words of mouth are delivered to the participants from Hamilton to Tonga through electronic devices and the messages are returned from Tonga to Hamilton. The principle remains the same and the only difference is the addition of 'e' (electronic) in front of *fanongonongo tokoto* to use emails, Facebook, Messenger, Zoom, and other online connections.

4.2 Survey Questions

Initially, eleven questionnaires were originally prepared for the purpose of face-to-face interviews with the survey participants in Tonga. Details of these questionnaires are summarised as follows:

- 1a - Demographic questions English version
- 1b - Demographic questions Tongan version
- 2a - Questions for Government organisations English version
- 2b - Questions for Government organisations Tongan version
- 3a - Culture questions English version
- 3b - Culture questions Tongan version
- 4a - Questions for church leaders English version
- 4b - Questions for church leaders Tongan version
- 5a - Questions for financial organisations
- 6a – Cyber grooming questions English version
- 6b – Cyber grooming questions Tongan version

Execution of the eleven questionnaires was expected to be implemented by the researcher through face-to-face interviews with the survey participants in Tonga. Because of the border restrictions, there was no opportunity to travel to Tonga and no opportunity to deliver these questions. As a result, the number of questionnaires was reduced to fit with the new e-ft methodology.

After online pre-discussions and verbal agreements with officials who were eager to assist in the survey, participants agreed and requested to send the questionnaires through emails to answer the questions and deliver to other participants. More than two hundred questionnaires were sent in August 2020. After a considerable period of time with no response from many participants some five hundred survey participants were contacted. The survey participants responded that they were still trying to complete the answers and would be returned upon completion. By the end of February 2021, (6 months), there were no responses from the survey participants about the questionnaires.

Due to unresponsiveness from survey participants, major amendments took place in the questionnaires. Priority questions were re-ordered and some questions were amalgamated with others. The result of new amendments had been reduced from eleven to five questionnaires as summarised below.

- 2a - Questions for Government Organisations English Version
- 2b - Questions for Government Organisations Tongan Version
- 3b - Culture Questions Tongan Version
- 6a - Cyber Abuse Questions English Version
- 6b - Cyber Abuse Questions Tongan Version

English and Tongan versions of the questionnaires (except the Culture Questions) were delivered to the survey participants using e-ft methods. Participants were asked to choose the easiest version to answer in either English or Tongan language.

4.3 Methods of e-fanongonongo tokoto (e-ft)

To implement e-ft, there were two basic questions applied. 1) How to communicate with the survey participants? 2) What are the questions to ask the survey participants?

1. How to communicate with the survey participants?

The e-ft communication methods were undertaken to connect with the Tongan survey participants: Facebook, Facebook Messenger (FM), email, and Zoom.

4.3.1 Facebook Messenger (FM)

Facebook Messenger (FM) was an effective communication tool to make initial contact with the survey participants. An initial message had been sent to families,

friends, and non-friends to explain the reasons for communication. There were no issues with the existing Facebook friends as most of these individuals are familiar and responded instantly to the initial message. However, non-Facebook friends responded promptly and offered to assist and partake in the survey. Another second message had been delivered to explain the intention to come to Tonga to conduct a face-to-face interview but unavailable due to the COVID-19 pandemic and border restrictions. Participants were asked to provide email addresses if they agreed to contribute/support this survey. Also, they were asked to choose the best method of communication: Zoom, FM, telephone, or Email.

In response to the participants' reply in the first/second contact, a third message was delivered with attachments: a pre-prepared letter to explain the purpose of this research, approval from the GoT, ethical approval from the UoW, and other related information delivered through FM or emails. Almost 95% of respondents replied effectively showing their willingness to support and partake in this survey and requested to send the questionnaires through FM and emails. A fourth email was send with the actual questionnaires being attached and delivered with advice on how to answer the questions.

Some of the answers in the answer sheets that were returned from the survey participants were unclear. Another message was sent to these individuals through FM and emails to clarify the unclear answers. In response, the participants responded and wrote the updated answers via emails and FMs. Other participants responded through face-to-face discussion on FM to solve the unclear issues.

4.3.2 Email

In trying to connect with the Tongan Government Ministries, an email was initially sent to the Prime Minister Office (PMO) requesting to provide email addresses of CEOs and IT representatives. A senior official from the PMO responded promptly with a list of contact emails and names of officials from each company to enable contact to be made.

A second contact via Email had been sent to respective CEOs to explain the purpose of this research and requesting their participation in this survey. Approval from the GoT and ethical approval from the UoW was attached to the email mailout. Some of the CEOs and government representatives responded promptly while others not

so. Those who agreed to participate in the survey requested to send the questionnaires through emails.

A third email was delivered with the attachments of questionnaires (Tongan and English versions) together with the Participant Information Sheets. Again, the survey participants were advised to choose the easiest forms, either the Tongan or English versions, to fill in. The questionnaires were open and free for other participants within the company/ministry to partake in this survey.

4.3.3 Zoom

All the civil servants and government officials had been invited to communicate using Zoom. Zoom is more advantageous as it is easy to set up and be able to communicate face-to-face. The purpose of the Zoom meeting was to clarify the aim and purpose of the survey. All the participants were mainly asked other questions (cybersecurity) and requested to send questionnaires via email. It was more convenient for the participants to take time to answer the questions.

4.3.4 Face-to-face interview on Messenger

The deployment of Facebook Messenger (FM) was an opportunity to face-by-face interview with the participants. The researcher and participants made use of the opportunity to share and raise queries about the questionnaires. The queries raised from participants were duly answered and participants were satisfied.

An opportunity arose to face-to-face interview one participant who was unable to read and answer questions in the questionnaire. This participant was not able to understand the procedure to access the internet. The wife assisted the participant (husband) to top up the telephone credit balance and set the FM to communicate with overseas friends. The interview was carried out successfully, and it was an opportunity to collect data from an ICT illiterate individual.

2. Types of questions to ask the survey participants.

The questions were broken down into multiple sub-questions to align with the thesis topic. The main structural content of all the survey questions relies on three main research questions summarised below:

1. *How has rapid ICT deployment in Tonga influenced online vulnerabilities?*

2. *How has the incidence of malicious cyber-events in Tonga exacerbated by aspects of Tongan culture?*
3. *What strategies have been identified by the research to improve ICT security in Tonga?*

The questionnaires delivered to the participants cover three main areas which are questions for:

- Government Ministries, Organisations, Boards, Financial Institutions, Schools, Businesses, Private Sectors, Embassy, People and Youths Questions – the main contents of this questionnaire covered the cybersecurity area intending to investigate the possibility of cybersecurity vulnerabilities in Tonga.
- Cyber-grooming Questions – the target participants were limited to non-married females only. The purpose of this questionnaire was to investigate the contacts from foreigners or outsiders to make friend requests with the target participants. To check for the outcome of these incoming friend requests whether for real or fraudulent purposes.
- Culture Questions – to search for the impact of ICT technology on Tongan values and other cultural concepts. Cultural values of Tongans are *faka'apa'apa* (respect), *lototō* (humility and generosity), *tauhi-vā* (loyality and commitment), *mamahi'ime'a* (sense of responsibility and commitment to the cause), and '*ofa* (love). Religion, culture, language, and other unrelated cybersecurity questions were included in the questionnaires.

The Cultural Questionnaire used the Tongan language only. As the major parts of the cultural questionnaire were open questions with more spaces to write the answers, the written answers needed to be clear and comprehensible. The important part of this question is the involvement of Tongans residing in Tonga and those living overseas. One intention is to bring the views of Tongan citizens from the outside world to compare with those living in Tongan.

Three types of questionnaires were delivered to the participants that covered the major areas of cybersecurity, non-cybersecurity, culture, and religion. In addition, the questionnaires were designed to reach a range of ICT literacy levels and for the participants that using the ICT devices such as desktop, laptop, iPad and mobile phone.

4.4 Data Collection

4.4.1 Physical copies vs e-copies

There were several contact points in Tonga where these citizens voluntarily offered their time and costs to assist in delivering/collecting the questionnaires to/from the participants. The contacted individuals were reliable and well known with secure jobs and respected positions within the Tongan community and government ministries. In this context, these citizens are regarded as Good Samaritans (GSs). Without any financial support and donation from the researcher, these GSs offered not only to deliver questionnaires via emails but also print out hard copies and delivered to each participant with their own time and costs.

No major issues were encountered with e-copies as respective participants saved the survey files in their respective laptops/desktops and emailed back the completed answers to the researcher in New Zealand. The printing out of physical copies, the delivery to the participants, and the returning of answers were carried by GSs. Participants with low ICT skills preferred to pass on the physical copies of the answers to GSs for final delivery to New Zealand. Participants who are unable to scan (due to the cost involved with scanning of all documents) also preferred to return the completed answers to GSs. The GSs then sent back the answers (both electronic and physical copies). Other participants preferred to take photos or scan by using smartphones and send them to the researcher via FMs or emails.

One of the advantages of sending the questionnaires to GSs is that both the researcher and survey participants did not meet each other. There was no direct communication between the researcher and the survey participants. Most delivery tasks relied on the GSs. Survey participants had the freedom to fill out the answers in the questionnaires as both the researcher and the survey participants never knew each other.

One GS collected the answers and travelled to the airport and asked one of Air New Zealand's passengers to hand-carry physical files of the participants' answers. The GS then contacted the researcher to give the time, date, mobile phone, name, and address of the passenger in Auckland. After 14 days of COVID-19 quarantine in the isolation area, the passenger was released to join the family on Wednesday 21st

October 2020. On the next day Thursday 22nd, the researcher travelled from Hamilton to Hillsborough Auckland to collect the questionnaire from the passenger.

4.4.2 Main issues of data collection

Despite technical and financial issues of delivering and returning hard copies, one of the other major issues entailed empty promises. An expectation of around 200 to 300 participants to partake in this survey based on previous contacts and arrangements. Participants from Tonga voluntarily offered their assistance and requested to send the questionnaires.

The questionnaires were sent to them (friends, families, non-friends, government officials, and more citizens) via emails and FMs with an expectation that the questionnaires would be completed. About 95 percent of questionnaires were delivered in August, September, and October 2020. The second week of February 2021 was the closing date with approximately less than 50 percent of the answers returned. Emails and FM contacts asking to return the questionnaires, but repeated responses replied: *te u ʻoatu ʻa pongipongi, te u ʻoatu he uike kahaʻu*/ (will send it tomorrow, will send it next week, and so on). Many potential participants made promises but didn't complete the questionnaire.

4.4.3 Advantages of e-ft

During the COVID-19 pandemic lockdown, the e-ft methodology is considered the appropriate solution. An online survey, such as Google Forms, is inappropriate because it removes cultural connections. Hard copy means everyone (survey participants) can access the questionnaires. Being more indigenous means more connecting and less impersonal. Despite the unavailability of face-to-face with others, there is a cultural connection between the survey participants and the researcher, a virtual sense of connectedness, humbleness, sharing, love, and willingness to assist. This connection stimulates the participants' hearts to answer the questions. Their answers were coming from their hearts.

Other significant factors were involved to ensure data collection is unbiased. These factors are the ages, regions, genders, communities, and social status. The ages of the participants ranged from sixteen to seventies. Males and females were proportionally enrolled. The five regions of Tonga were all involved in data collection and reached out to youth, churches, NGOs, businesses, and other

organisations. Other participants from government officials, Ph.D. scholars, church leaders, and the lowest level of society have participated. The entire demographic structure enrolled in this survey.

4.4.4 Disadvantages of e-ft

The e-ft original target is to collect more than five hundred participants. This target is based on a face-to-face interview with the survey participants. The researcher believes that the more people involved, the better the research is. Gaining a large number of survey participants reduce the risk of biased decision and increase the tendency for accuracy, especially in decision-making. A large amount of data collection provides more reliable and stronger results because they have a smaller margin of error.

There is a limitation in data collection. The number of target participants was not achieved (*see Figure 21*). A very clear reason as previously mentioned, the COVID-19 pandemic and travel restrictions altered the original plan. Because of these reasons, the researcher and the project supervisors agreed to proceed with the e-ft methodology. A decision was made to utilize the maximum number of participants possible from the e-ft methodology and fully analyze this data. Border restrictions and uncertainty meant it was impractical to continue waiting to return to Tonga.

4.4.5 Total number of survey participants

The table below summarises the total number of survey participants, the methods deployed to collect the data, and the weekly responses from the participants. The disbursement of survey questionnaires started in August 2020 and closed in February 2021. The methods of collecting survey answers were emails, messenger, hand-carry, and interviews via Facebook messenger. The chief supervisor and the surveyor have agreed to proceed to the next phase (data analysis) with the number of answers collected.

				Weekly Records of Data Collection											
Emails															
	Aug-20		**Sep-20**		**Oct-20**		**Nov-20**		**Dec-20**		**Jan-21**		**Feb-21**		**Total**
	Week 1		Week 1	4	Week 1	7	Week 1	11	Week 1		Week 1		Week 1	1	23
	Week 2		Week 2	2	Week 2	7	Week 2	12	Week 2	13	Week 2	3	Week 2		37
	Week 3		Week 3	4	Week 3	5	Week 3	7	Week 3	11	Week 3		Week 3		27
	Week 4	5	Week 4	4	Week 4	2	Week 4	1	Week 4		Week 4		Week 4		12
	Week 5	2	Week 5	3	Week 5	8	Week 5		Week 5	3	Week 5		Week 5		16
Messenger															
	Week 1		Week 1		Week 1		Week 1	1	Week 1	1	Week 1		Week 1		2
	Week 2		Week 2		Week 2		Week 2		Week 2	2	Week 2		Week 2	10	12
	Week 3		Week 3	1	Week 3		Week 3		Week 3	1	Week 3		Week 3		2
	Week 4		Week 4		Week 4		Week 4		Week 4		Week 4		Week 4		0
	Week 5		Week 5		Week 5		Week 5		Week 5		Week 5		Week 5		0
Others															
Hand-carry from Tonga						7									7
Face to face interview on Messenger										1					1
															139
Total Participants		**7**		**18**		**36**		**32**		**32**		**3**		**11**	**139**

Figure 21: Record of data collections

Figure 21 represents the total number of survey participants who participated in the survey. The total number of participants who took part in this survey was 139 individuals. About eighty-eight (88) represent the Tongan people; thirty-one (31) belong to the government organisations; fifteen (15) represent Tongan culture, and five (5) belong to the cyber-abuse category.

CHAPTER FIVE

5. DATA ANALYSIS

All the answers collected from the survey participants together with all the questions in the questionnaires were converted from Word documents to a 2016 Excel spreadsheet. To carry out the tally process, the first step involved the copy of all the questions from Word documents and pasted them onto spreadsheets. Instead of using the participants' names to input answers, ID numbers were placed on each column to the right side of the questions starting from the first to the last participants. Only the researcher knows the names of the participants in terms of their respective IDs.

5.1 Demographic Analysis

5.1.1 Language and gender

The total number of survey participants who partook in the survey was 139 individuals. Out of the 139 participants, 57% (79 participants) were male and 43% (60 participants) were females. Survey questionnaires were delivered in English and Tongan versions and participants were free to choose the favoured language to answer the questions. The majority (58%) (80 participants) favoured writing in English while 40% (56 participants) chose to answer in Tongan. The remaining 2% (3 participants) preferred to answer both Tongan and English.

5.1.2 Age

Participants' ages were categorised into six main divisions (16-20, 21-30, 31-40, 41-50, 51-60, and 61-70) starting from 16 up to 70 years of age. *Figure 22* shows the number of participants within each age category.

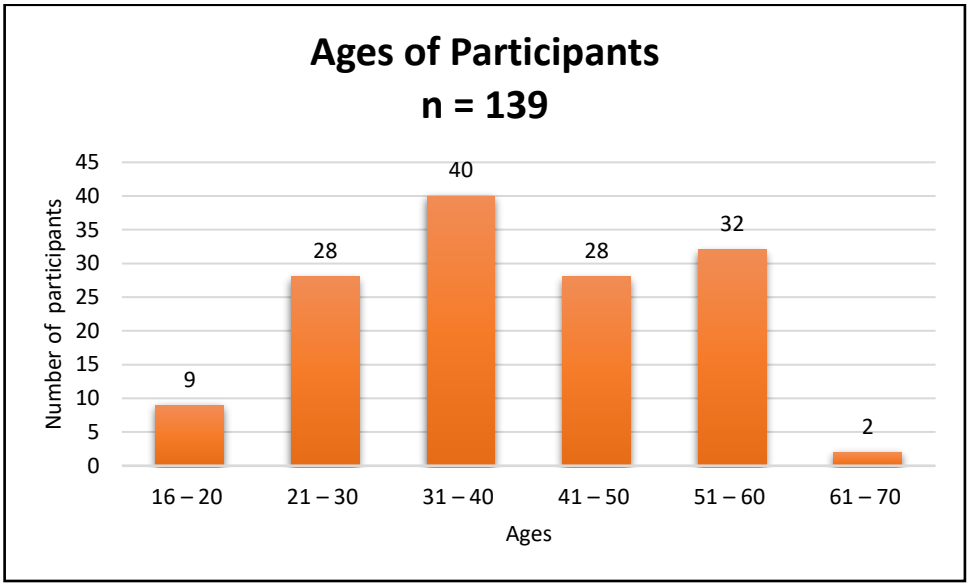


Figure 22: Ages of survey participants

The highest portion, 29% (40 participants) of the survey participants' ages was within 31 – 40 years followed by 23% (32 participants) within 51 – 60 ages. The categories 21-30 and 41-50 tie in 20% each with a total number of 56 participants (28 each). The remaining 8% was shared between 16-20 (7%) (9 participants) and 61-70 category (1%) (2 participants).

5.1.3 Regions

Table 11 summarises the regions of where the participants came from and the number of participants who answered the questions from each category (GoT, Culture, and Cyber-Abuse). Details of Tonga's regions are summarised in Tonga's Map (see Section 2.3 – *Figure 7*).

Table 11: Participants' Regions

Region	People	GoT	Culture	Cyber-Abuse	Total	Percent (%)
Tongatapu	57	25	3	4	89	64%
Vava'u	16	6	8	1	31	22%
Ongo Niua	8				8	6%
Ha'apai	6				6	4%
Overseas			4		4	3%
'Eua	1				1	1%
Total	88	31	15	5	139	100%

The majority (64%) (89 participants) of the participants came from Tongatapu, followed by 22% (31 participants) from Vava‘u. Both (Tongatapu and Vava’u (86%) (120 participants) are the two main islands in Tonga. The remaining 14% (19 participants) shared amongst the other regions include Ha‘apai, ‘Eua, Ongo Niua, and overseas.

5.1.4 Computer Devices to access internet

An open question asked the survey participants to list all the computer devices that they used for communication (see Question 7 in *Appendix* 10). There are multiple choices of answers and allow to choose more than one answer as according to the computer devices used. The total number of choices for this question was 363 which summed up the total number of computer devices operated by participants.

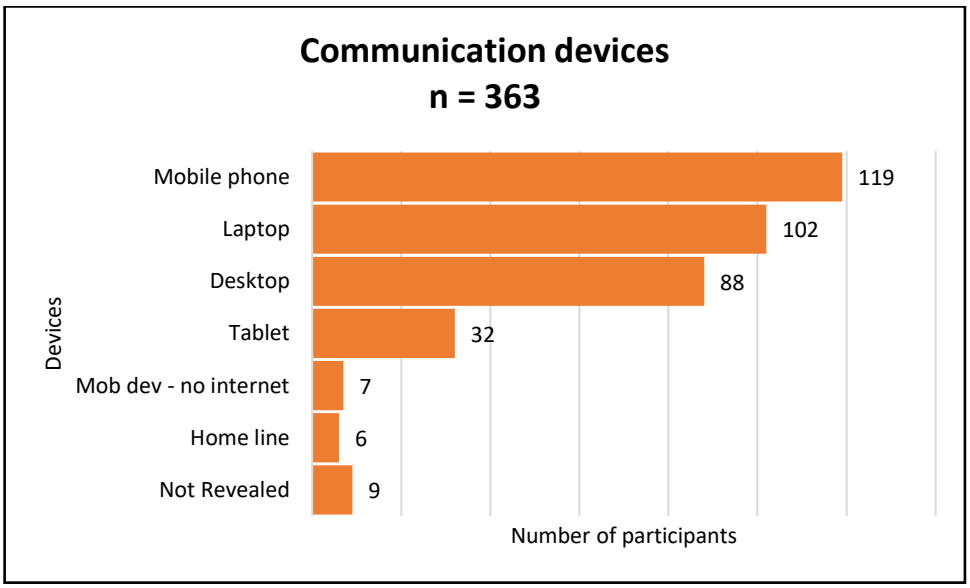


Figure 23: Communication Tools

Figure 23 summarises the total number of devices used for communication. The top three devices operated by the Tongan participants were mobile phones, laptops, and desktops. The highest portion, 33%, (119 participants) deployed mobile phones, followed by laptops, 24%, (102 participants). In the third position, 24% (88 participants) used computer desktops followed by tablets, 9%, (32 participants) in the fourth position. The remaining 22% shared amongst mobile devices without accessing the internet, traditional home-line phones, others preferred not to answer this question.

5.1.5 Participants' categories

Table 12 reveals the participants from each category. The highest portion, 39%, (54 participants) represented the GoT ministries, followed by 18% (25 participants) from Schools. About 17% (24 participants) came from Youth. The remaining 26% (36 participants) were shared amongst Public Enterprises, Church, Private Sector, Bank, Agency/Body, Aid Agency, and Others. Others refer to school leavers, ICT grassroots levels, mothers, and participants that preferred not to answer this question.

Table 12: Participants' organisation categories

Organisation	People	GoT	Culture	Cyber-Abuse	Total	Percent (%)
Government Ministry	42	11	1		54	39%
School	11	7	7		25	18%
Youth	16	2	1	5	24	17%
Individual	9	1			10	7%
Other	7		2		9	7%
Public Enterprise	1	3	2		6	4%
Church	2		1		3	2%
Private Sector		3			3	2%
Bank		2			2	2%
Agency/Body		1	1		2	1%
Aid Agency		1			1	1%
Total	88	31	15	5	139	100%

5.1.6 Participants' income

An open question (see Question 9 in *Appendix* 10) was asked about participants' sources of income. A multiple-choice question and participants were asked to choose more than one answer depending on different sources of income received. The total number of answers for this question was 159. A total of 67% (107 participants) earned income mainly from wages/salary from the GoT, churches, and other ministries/organisations. Farm's income represented 11% (17 participants) followed by 'Other' income in third place (10%) (16 participants). 'Other' refers to home caretakers, consultants, and participants that refused to answer the question. About 4% (7 participants) main income earned from fishing and weaving. *Table 13* represents the summary of participants' income.

Table 13: Source of income

Income	People	GoT	Culture	Cyber-Abuse	Total	Percent (%)
Wages/Salary	66	23	14	4	107	67%
Farm	12	2	3		17	11%
Other	10	5	1		16	10%
Overseas Remittance	8	2	1	1	12	8%
Fishing	3	1	1		5	3%
Weaving	2				2	1%
Total	101	33	20	5	159	100%

5.1.7 Participants' income per annum

Table 14 summarises the annual incomes of the survey participants. The highest portion, 51%, (69 participants) earned annual income between T$10,000-T$40,000. Secondly, 13% (17 participants) earned income between T$40,000-T$70,000 followed by 8% (11 participants) earned between T$7,000-T$10,000. The remaining 28% (27 participants) earned income within other ranges.

Table 14: Annual earnings

Amount (TOP T$)	People	GoT	Culture	Total	Percent (%)
More than T$1M	2			2	1%
More than T$100,000		2	2	4	3%
T$70,001-T$100,000	1	3	1	5	4%
T$40,000-T$70,000	8	8	1	17	13%
T$10,000-T$40,000	49	13	7	69	51%
T$7,000-T$10,000	7	2	2	11	8%
T$4,001-T$7,000	5			5	4%
T$1,001-T$4,000	7	1		8	6%
Less than T$1,000	4			4	3%
Other/no answer	5	2	2	9	7%
Total	88	31	15	134	100%

5.1.8 Participants' qualifications

Table 15 represents the qualifications of participants. The majority, 30%, (42 participants) gained Bachelors' degrees followed by 27% (37 participants) who gained Diploma's qualifications. With higher qualification, 16% (22 participants) gained Masters' degrees, and 6% (9 participants) achieved PhDs. The remaining

21% have No qualifications, Certificates, Postgraduate, and Others or did not answer the question.

Table 15: Participants' qualifications

Qualification	People	GoT	Culture	Cyber-Abuse	Total	Percent (%)
Doctorate (PhD)	2	5	2		9	6%
Master	11	9	2		22	16%
Postgraduate		1			1	1%
Bachelor	30	9	2	1	42	30%
Diploma	22	7	7	1	37	27%
Certificate	3		1		4	3%
No qualification	15				15	11%
Other/no answer	5		1	3	9	6%
Total	88	31	15	5	139	100%

5.1.9 Demographic Analysis Summary

The majority, 86%, (120 participants) of the participants came from Tongatapu and Vava'u, which are the two main regions in Tonga. These two provinces are the centre of ICT development in Tonga, especially Tongatapu, the capital of Tonga.

The participants' ages range from 16 – 20 up to 61 – 70 years of age. All the ages (16-20, 21-30, 31-40, 41-50, 51-60, and 61-70) were able to participate in the survey. The highest portion, 29%, (40 participants) who contributed to the survey came from the 31 – 40 years of age's group.

Mobile devices and laptops are noted to be the most affected computer devices discovered in this research. About 62% (226 participants out of 363), operated mobiles and laptops. This figure reflects the ICT transfiguration of communication from large computers to portable devices.

About 58% (80 participants) were able to read and answer the questions in the English language. This high portion can be a measuring tool for the literacy and academic status of Tongans. Also, about 83% (115 participants) achieved academic qualifications ranging from Certificates up to master's and PhD levels.

According to the annual income, the highest portion, 51%, (69 participants) of the survey participants' annual income fell within the category of TOP$ 10,001 – TOP$

40,000 per annum. (ANZ foreign exchange rate as of today, Monday 19th April 2021, is 0.59 cent (ANZ, 2021)). To convert the annual income of TOP$ 10,001 – 40,000 to NZ currency is an equivalent of NZD$ 5,900 – NZD$ 23,600 as the average income of the participants.

5.2 Cybersecurity Analysis

5.2.1 Contacted by Scammers

A question asked the participants (see Question 14 in *Appendix* 10) if they had contacted or came across any lured bait from cyberattacks, such as phishing emails, fake antivirus software, fake websites, credit card, lottery scams and so on. The focal point of this question is not directly related to the victims who were already involved in scams like losing money or credentials but to investigate the number of participants that were contacted but not victimised by cybercriminals.

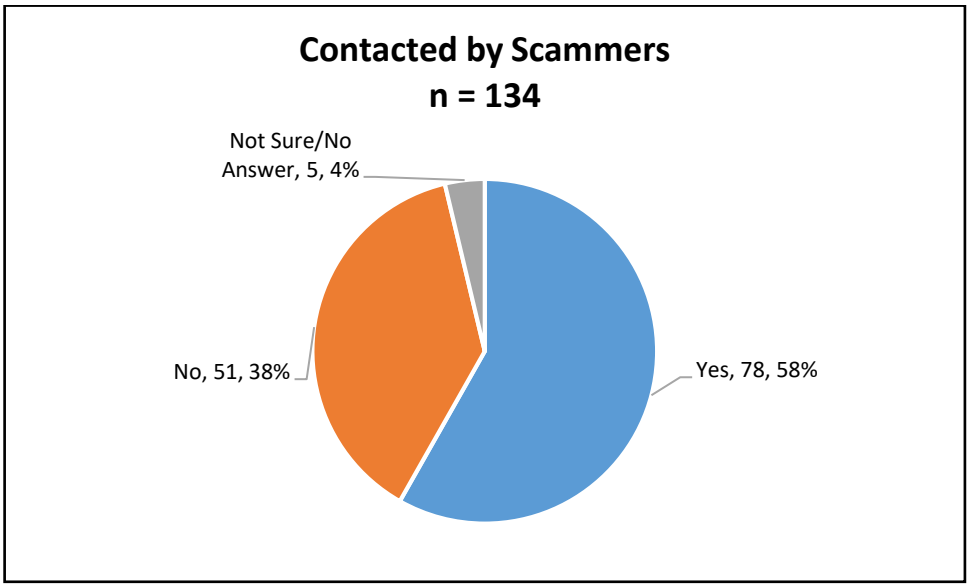


Figure 24: Contacted by cyberattacks

The target participants (n = 134) were from the people and the GoT ministries, businesses, private sectors, schools, financial institutions, public enterprises, aid agencies, churches, and other organisations. As mentioned previously, the total number of survey participants involved in this research was 139. About five participants missed out on this question as they belonged to the cyber-grooming section. The cyber-grooming participants were only for single unmarried females, with another section with a separate questionnaire specifically assigned to them.

Figure 24 reveals that the highest portion, 58%, (78 participants) came across contacts from cyberattacks. This means that participants received contacts from scammers through different types of online contacts but no lost money or credentials. About 38% (51 participants) never came across any contact and 4% (5 participants) provided 'No Answer/Not Sure' to this question.

Concerning this issue, one of the civilians wrote to express concern about fraudulent emails that happened within one of the GoT's ministries. The civilian stated that: … there is a scam in our work emails where we received emails from our employees but different and unfamiliar email addresses. Also, when we send emails to employees outside our work, they do not receive them, or they will receive them more than three times. While on our site, our emails bounced back and said it is undelivered.

5.2.2 Other victims known by participants

A question asked (see Question 15 in *Appendix 10*) if the participants knew other people that had been attacked or involved in OS. The answer for this question is shown in *Table 16.*

Table 16: Other victims of OS known by participants

Answer	People	GoT	Total	Percent (%)
Yes	42	21	63	53%
No	36	7	43	36%
Not Sure/No Answer	10	3	13	11%
Total	88	31	119	100%

There were 119 participants involved, (88 participants from GoT and 31 participants from people categories) and answered the question. Again, the participants from cyber-grooming and culture categories were not involved in this question as separate questions were allocated to them. About 53% (63 participants) knew other Tongans already involved or being attacked while 36% (43 participants) did not know any people involved in OS. The remaining 11% (13 participants) given 'Not Sure/No Answer' to this question.

5.2.3 Number of contacts from scammers

A question asked (see Question 16 in *Appendix 10*) for the number of contacts made from the scammers. Specifically, this question looks for the number of times (such as once, twice, or more) did the scammer contact. About 119 participants answered this question.

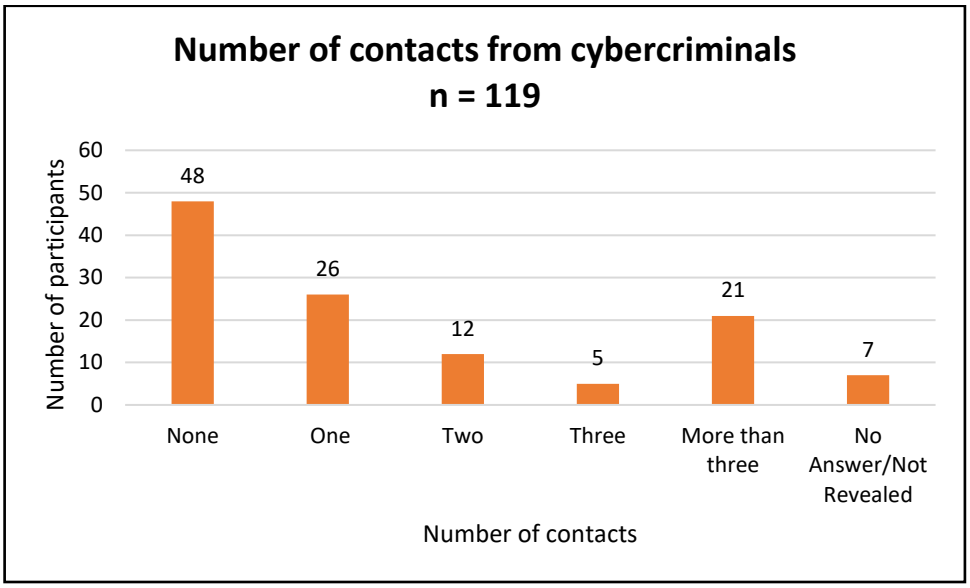


Figure 25: Number of cyberattack contacts

Figure 25 reveals the highest portion, 40%, (48 participants) were never involved in contacts from cybercriminals. About 18% (21 participants) had been contacted more than three times, while 22% (26 participants) were involved in one-time contact. Also, 10% (12 participants) were contacted two times and 4% (5 participants) three times. Finally, 6% (7 participants) disagreed/did not reveal the answer to this question.

5.2.4 Number of victims who lost money to scammers

A sensitive question: *Did you lose any money?* was asked (see Question 17 in *Appendix 10*). Despite the sensitive and straightforward nature of the question, some of the victims stepped forward to give their answers while others refused. The participants who refused to answer this question were from government ministries that related to the privacy and secrecy of the organisation.

Although 12% (15 participants) shown in *Figure 26* refused to answer this question, others preferred to take this challenge. The highest proportion, 76%, (90 participants) did not lose money while 12% (14 participants) were involved in

cyberattacks and lost money to scammers. Details of the answers show in the pie graph below.

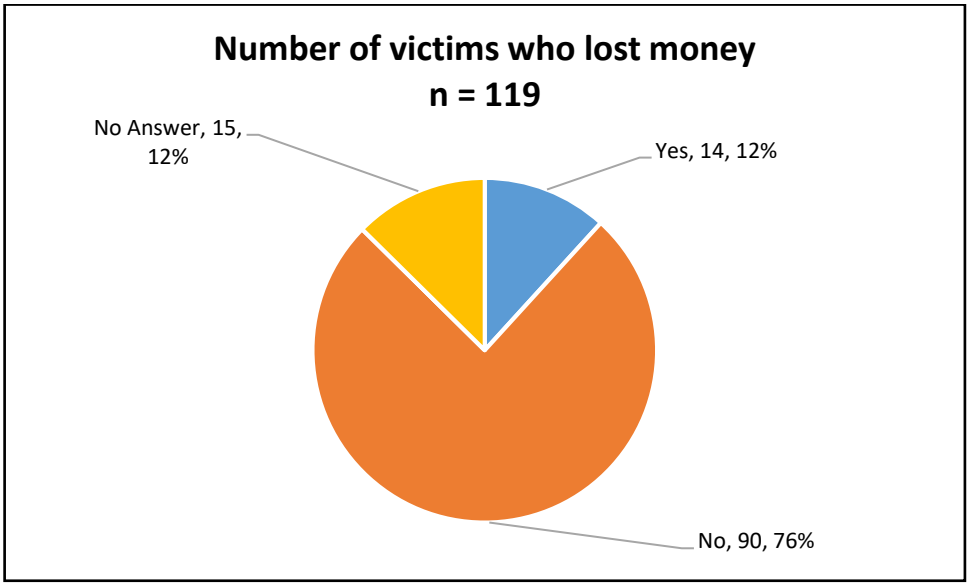


Figure 26: Total number of victims who lost money to cyberattacks

The information provided below are some of the quotes from the survey participants that were contacted by cybercriminals (see *Appendix 3* for more quotes from victims).

- I didn't know about it until I checked my account balance and found out that there was money being taken from my account when I was in Tonga. At the time that the scamming happened, I was in Fiji. I contacted our bank here in Tonga, and they informed me that it was a scam and will advise me when they sort everything out. After a few weeks, they informed me that they were able to trace the hacker, and they were responsible to return my money.
- *Email mai he'eku kei ako i Port Vila Vanuatu talamai ke totongi ange US$300 ka e ma'u mai 'e ku US$1,000. Mole 'e ku seniti …, pea u 'ita ho no kaka'i au pea kou ako foki ai*. [translation by author] Received an email when I was studied in Port Vila Vanuatu to inform me to pay US$300 with a payment of US$1,000 to be received later. I lost my money … I was so angry for deceiving me and learned from this error.
- They asked to provide some information about my visa card… they said it was free of charge. I found they charged me $100+ from my account.

- *Na‘e tā mai e Pangike ‘o talamai tenau hold e pa’anga ‘oku toho ‘aki ‘e ku kaati ‘i China. Neu ngaue‘aki ‘eku card ‘i Fiji lolotonga ‘eku ‘iai ki he toho sēniti. Ko ‘eku mahalo ia na‘e ‘ilo’i ai. Neu ilifia leva ke to e fakahū ha sēniti ki he‘eku account.* [translation by author] The bank called and said they would hold cash withdrawals with my card in China. I used my card in Fiji where I attempted to withdraw cash. I guessed that the scammer there discovered it. I was then terrified of depositing more money into my account.
- I clicked on a link which took me to a website of some stores in a foreign country… A form appeared for me to complete my name, D.O.B, address, and then credit card to transfer the money over to this account. I was only 13 years old; I did not understand credit cards. So, I stole my parents’ credit card and entered the required information….. It affected my health. My friend told me on the next day at school that his page got hacked and it scared me knowing I accepted a link from a stranger. That whole day, I could not eat, thinking about what happened and I was hungry, but I still did not want to eat. I also never told my family….. However, I found out that I used my mum’s expired credit card which gave me huge relief, but I was still very worried about opening my Facebook account.
- *Ne fetu‘utaki mai hoku kaungame‘a he email ko e kole tokoni $2,000 ki he‘ene ki‘i me‘a fakavavevave ka e toki toho e sieke laumano he ‘osi māhina ‘e taha pea toki taa‘i fakafoki mai ‘eku sēniti pea ne ‘omai mo e account ke sent ange ki ai pea ko e ngata pe ia ‘ema talanoa*. [translation by author] My friend emailed me and asked $2,000 to pay for an urgent matter. He (my friend) is expected to withdraw a thousand dollars cheque in one month and then deposited my money back. An account number was provided to deposit the money and since the money was deposited to the account no more contact was ever made.

5.2.5 Amount of money lost to cyberattacks

With the 14 participants (mentioned in *Figure 26*) who lost money, the majority (12 participants) stepped forward to give the amount of money lost to cyberattacks while others (2 participants) denied answering the amount lost. The denial to state the amount of money lost was due to personal privacy and secrecy.

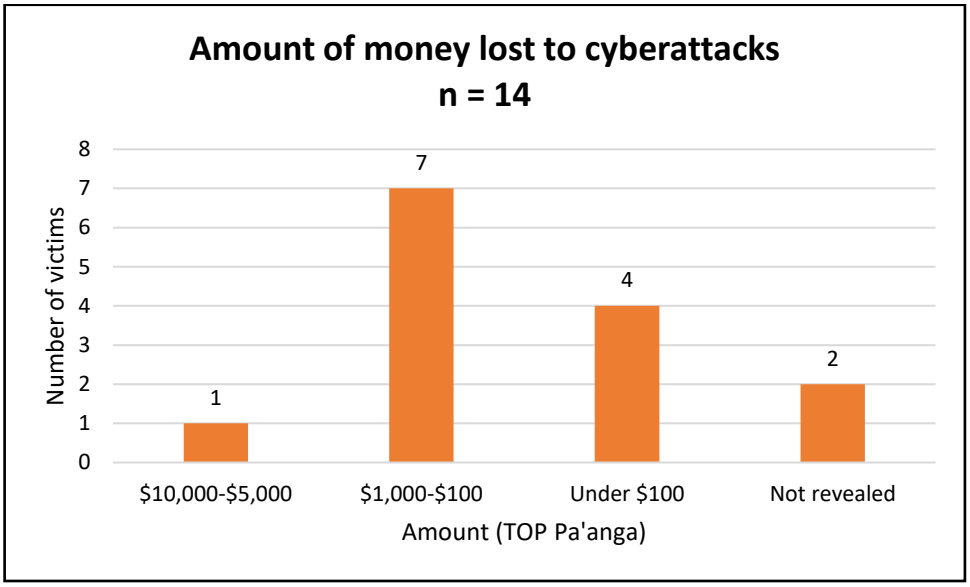


Figure 27: Amount of money lost

Figure 27 summarises the number of victims together with the amount of money (TOP$ Pa‘anga) lost to cyberattacks. About 7 participants lost money within the range of TOP $100- TOP $1,000 and 4 participants lost money under TOP $100 category. Two (2) of the participants denied giving the amount lost due to restriction and privacy. One victim lost an amount between TOP$ 5,000 – TOP$ 10,000 on one occasion in 2015 - 2018.

The victim who lost the most money stepped forward to report part of a story of how a large amount of money was lost from their family. One female member of the family left Tonga to go overseas on Recognised Seasonal Employer (RSE scheme) for the purpose of raising funds for purchasing a vehicle for children transportation to and from school. From overseas, the female member deposited the money (TOP$ 5,000 – TOP$ 10,000) to the hacker’s bank account. Since the money was deposited to the account, the family received no vehicle and no contact ever made with the scammer.

5.2.6 How scammers contacted people?

Online scammers distributed different ways of communication to contact with Tongan Innocents (TIs). A question asked; *How did they (scammers) contact you (participants)*? (see Question 27 in *Appendix* 10). The question allowed more than one answer for the participants to choose from. The total numbers of answers for this question were 115 (representatives from GoT and People only).

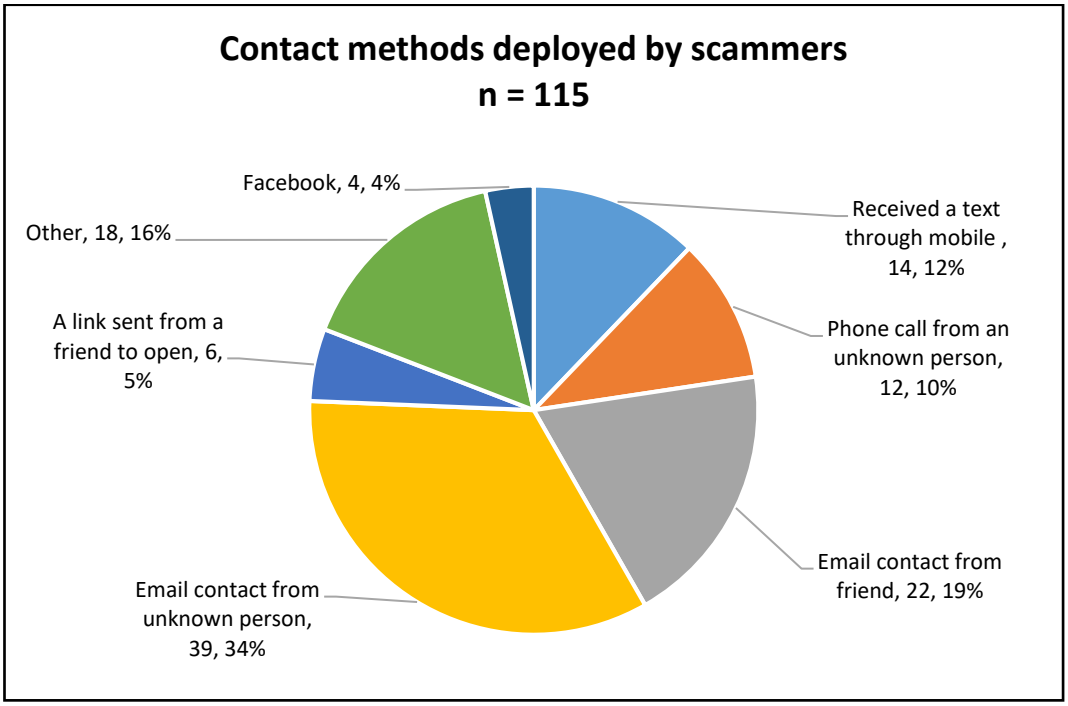


Figure 28: Communication methods delivered by scammers to Tongan Innocents

Figure 28 represents the delivery methods implemented by scammers to deliver fraudulent messages to Tongan Innocents (TIs). The top three (3) delivery methods were:

- Email contact from an unknown person – 34% (39 participants)
- Email contact from a friend – 19% (22 participants)
- Received a text through mobile – 12% (14 participants)

Other contact methods delivered by scammers were:

- Text from scammers using the mobile phone – 12% (14 participants)
- A phone call from an unknown person – 10% (12 participants)
- A link sent from a friend to open – 5% (6 participants)
- Contact through Facebook – 4% (4 participants)
- Other contacts – 16% (18 participants)

The first top two contact methods (as listed above) were both email contacts. Email from an unknown individual plus email contact from a friend were the two most effective methods of contact performed by the scammer to cheat Tongan people. The combination of these two methods, 34% ((39 participants) + 19% (22

participants)) revealed that 53% (61 participants) scammers deployed *email phishing to* contact Tongan people.

5.2.7 Information requested by scammers.

A question asked; *What sort of information did the scammer ask for?* (see Question 28 in *Appendix 10*). Multiple questions were delivered and asked participants to choose more than one answer for this question. A total number of 112 answers from the GoT and People replied to the question. Details of their answers are shown in *Figure 29*.

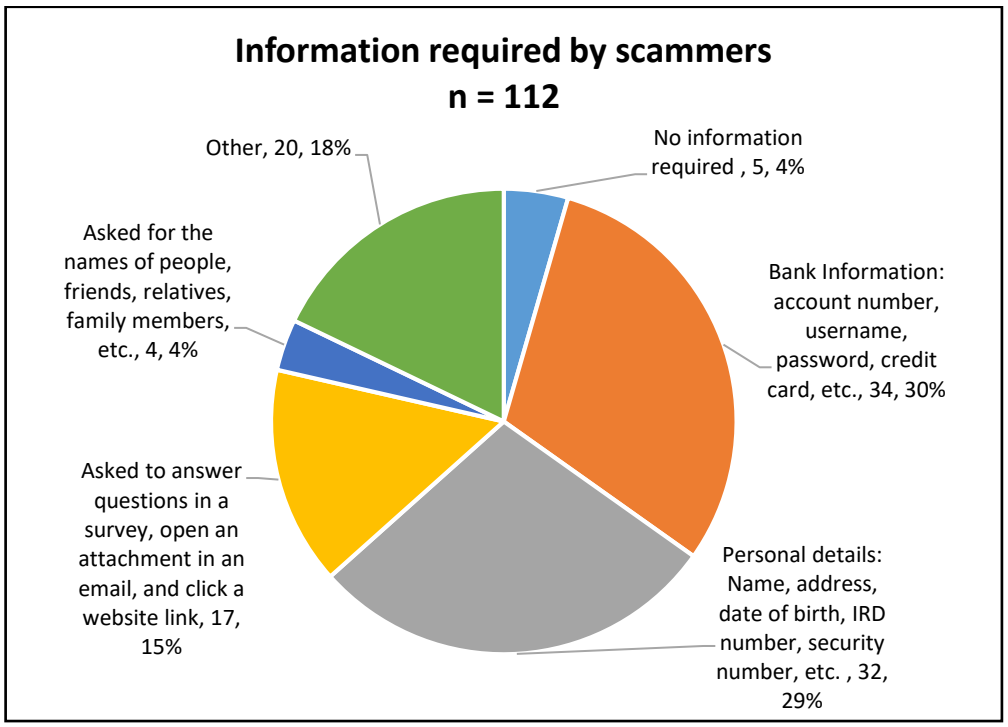


Figure 29: Information requested by cyberattacks.

Figure 29 reveals that scammers requested different types of information from the TIs to perform the cyberattacks. The four main types of information requested by scammers are listed below starting from highest to lowest percentage/number. These are;

- Asked the participants to provide bank credentials such as account number, username, password, credit card, and other private identifications – 30% (34 participants).
- Asked to provide other private details such as name, address, date of birth, IRD number, security number, and personal information – 29% (32 participants).

- Received requests to answer a question in a survey, open an attachment in a survey, and click on a website link – 15% (17 participants)
- Asked for the name of people, friends, relatives, and family members – 4% (4 participants)

5.2.8 Losing secret information to scammers

One of the sensitive questions asked (see Question 29 in *Appendix 10*). *Have you given your secret information to the scammer?* Only 66% (79 out of 119 participants (i.e., total numbers of GoT and People)) agreed to answer this question. Secret information refers to bank account number, username, password, credit card, name, address, date of birth, IRD number, security number, and other private credentials. Details of the answers are shown in the *Figure 30*.

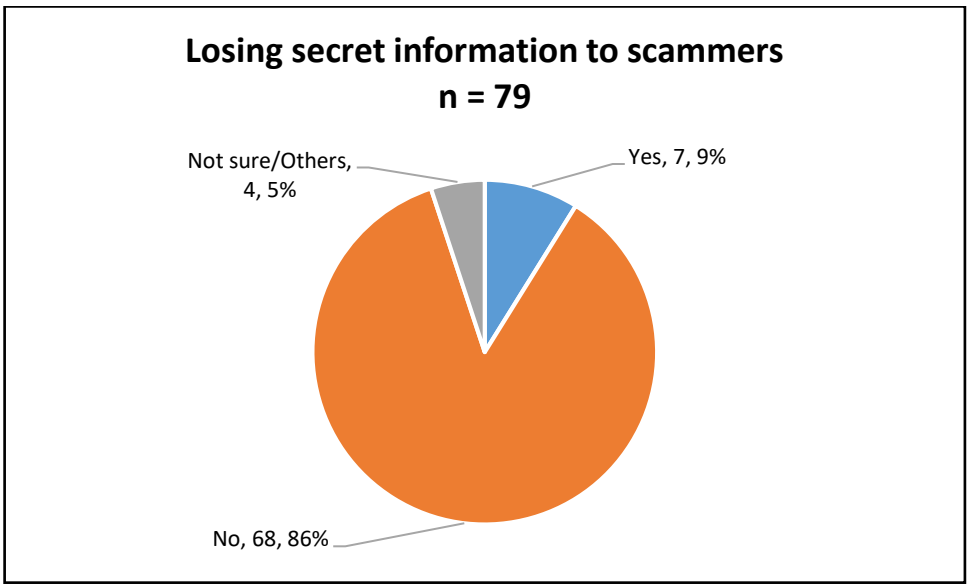


Figure 30: Losing sensitive information to scammers

The highest portion, 86% (68 participants) managed to keep their private information secret. About 9% (7 participants) of TIs failed to lure baits and resulted in giving their secret information to scammers. Besides, 5% (4 participants) were not sure and unable to answer the question due to privacy reasons.

Provided below are some of the quotes from the survey participants in relation to the question above. There are eight more quotes from the participants and they are summarised in *Appendix 3*.

- They promised to take the initial payment for software that I can use to make money. I entered my credit card details to make the payment and it took the payment and shortly after, the online conversation terminated and the person in contact took the money and never tried to reach me back.
- I was immature as I was only 13 years old …. I did not know enough about online scamming … so when the scammer asked about my personal information (in a formal manner), I just gave it thinking nothing wrong would happen.

- *Ne talamai ke fakahū ange ki he account pea tuai pe ho no fakahū atu e sēniti pea ʻikai ha to e felaveʻi mo e tokotaha ni*. [translation by author] The scammer advised me to deposit money to an account. As soon as the money deposited, no more contact with this person.
  - She sent me an email to inform me that I am one of the winners to apply for the US citizenship. Therefore, she needed me to send her US$ 1,000 to complete the requirement. I checked her email and the link she sent to me, it was fake. So, I didn't send anything.
  - They told me that they want to share their fortune with me – but I have to pay a small amount upfront.

5.2.9 Years of cyberattacks

A question asked (see Question 20 in *Appendix 10*); '*What year did the online scamming happen***?**' This question targeted to record the number of contacts from the scammers to the TIs. Some participants answered more than one answer, as they were involved in more than one cyberattacks in different years and different places. The total number of answers given by the participants from GoT and People was 85. Details are summarised in the *Figure 31* bar graph.

Refer to *Figure 31*, the most cyberattacks, 35%, (30 cyberattacks) took place in 2015 - 2018 followed by 21% (18 cyberattacks) in 2010 - 2014. Besides, there were two cyberattacks (2%) that occurred in 1990 - 1999 and one cyberattack (1%) took place before 1990.

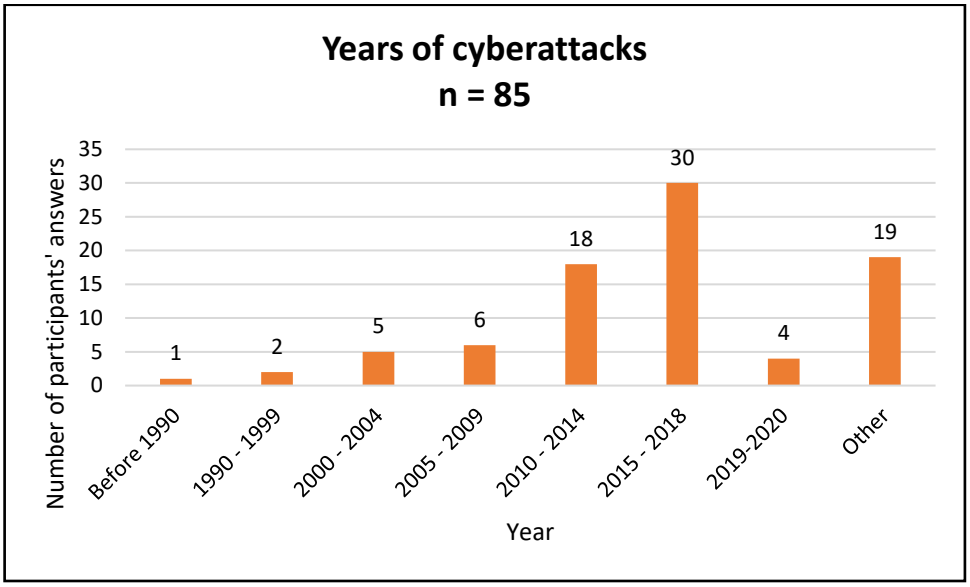


Figure 31: Years of cyberattacks

In summary, the total number of cyberattacks was 78% (66 cyberattacks) that took place before 1990 to 2020. The remaining 22% referred to as 'Other' which means that the participants that did not remember cyberattacking happened and also participants that disagreed to provide answers to this question. The answers provided include victims that lost money/credential information and other individuals that are contacted by cyberattacks where no money/credentials lost.

5.2.10 Time of cyberattacks

Another question asked (see Question 19 in *Appendix 10*); *What time did the online scamming take place?* Participants could pick more than one answer as cyberattacks occurred at different times and took place more than one attack for one victim. The majority 53%, (34 participants) were classified in the 'Other' category. 'Other' means for the participants that they were not sure of the time that cyberattacks happened and participants that provided no answer to the question. The remaining 47% (30 participants) agreed to give the time of the cyberattacks.

Cyberattacks happened in 24 hours, morning, afternoon, evening, and midnight as summarised in *Figure 32.* About 21% (13 participants) had attacked during the day from 6 am – 12 midday and 17% (11 participants) in the evening from 6.01 pm – 12 pm-midnight. Another 6% (4 participants) were attacked in the afternoon from 12.01 pm – 6.00 pm. The remaining 3% (2 participants) took place at 12 am-midnight – 6 am.

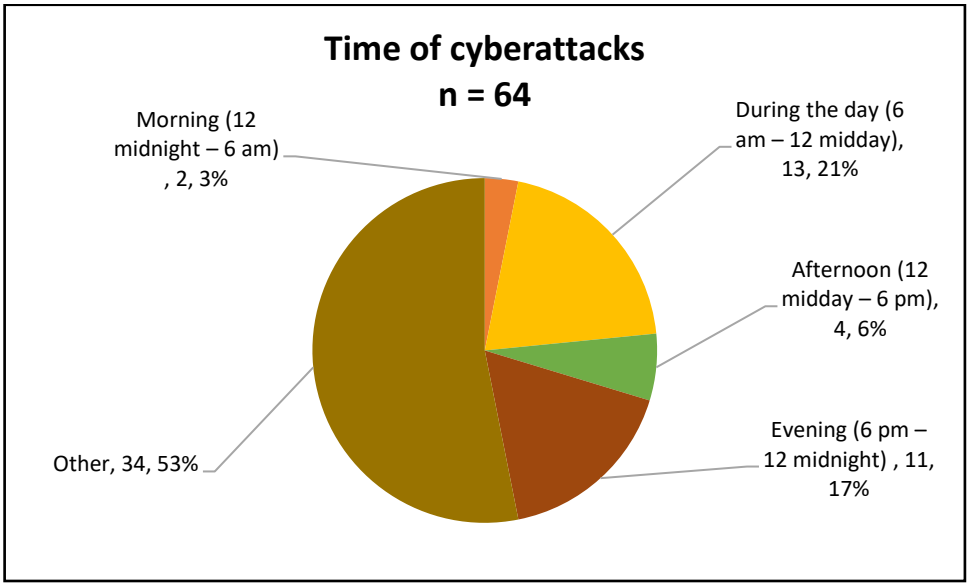


Figure 32: Time of cyberattacks

5.2.11 Cybersecurity workshop

A question asked about the enrollment in cybersecurity workshops (see Question 47 in *Appendix 10)**;*** Participants from the GoT and People (n = 119) were able to answer this question.

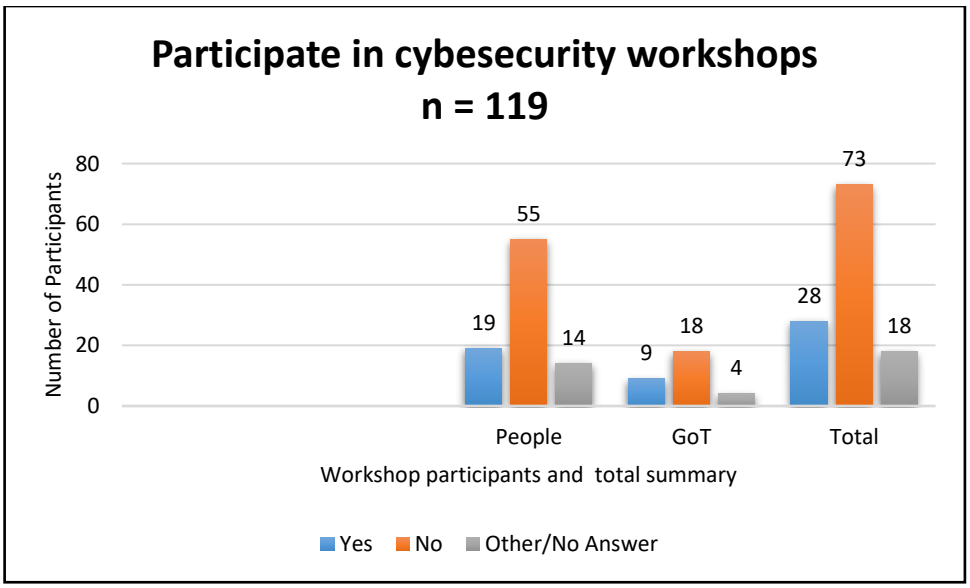


Figure 33: Participate in cybersecurity workshops

Figure 33 represents the People (P), GoT (G), and the Total (combination of P+G) number of people enrolled in cybersecurity workshops. In total, most (61%) (73 participants) people did not attend any cybersecurity workshop. Only 24% (28 participants) participated in some workshops, and the remaining 15% (18 participants left this question with 'Other/No Answer'.

5.2.12 Significance of Cybersecurity workshops and training

Another question asked the GoT's participants (n = 31) about the significance of cybersecurity workshops and training. *Do you think Tongan people need education or more workshops to assist in protecting themselves from the scammers*? (see Question 43 in *Appendix 10*). In response, the majority (97%) (30 out of 31 participants) said 'Yes' to support the idea of conducting workshops and training for the government employees. Only one participant (3%) did not provide an answer to this question.

Provided below is a comment from one of the survey participants about the importance of cybersecurity workshops and training. There are eighteen more quotes from the participants about this subject. These comments are summarised in *Appendix 5*.

- YES, and the Tonga government and people will need to wake up and take this cybersecurity issue very seriously. Everybody is accessing the internet and to be even worst social media. People go to social media and put up their photos and even post their problems or issues so when you read their profile you can even tell the story of her or his life background. As a woman, I am sometimes angry to see comments with language that encourages problems. I see girls texting or FB in church too and so Tonga in government, church, community, and school need to be aware of this and educate their citizens. We are losing a lot of our prestige in this technology life. People download the bible and hymns to use in church and then FB at the same time. There is no more holiness in the church and there is no more difference between Christians and heathen because everyone is accessible to the internet and honestly everyone is addicted. Sometimes I cook and call my husband to come and eat. He just looks down at his phone and eats without saying thank you to my beautiful cooking.

  Seriously, where are all our values of love and respect going now? The government needs to invest more in studies and on system or division in the government response to start this job of educating and helping people out from this.

5.2.13 Cybersecurity expert and qualification

Two questions were put together in one table. The purpose of these two questions is to find out the number of cybersecurity experts in government organisations (n = 31) and their academic qualifications. *Table 17* summarises the questions and the answers from the GoTs' participants only.

Table 17: Cybersecurity expert and qualification

Is there a cybersecurity expert in your organisation? (see Question 50 in ***Appendix** 10*)		
	GoT	**%**
Yes	4	13%
No	23	74%
Other/No Answer	4	13%
Total	31	100%
What qualification does your organisation's cybersecurity expert hold? (see Question 51 in ***Appendix** 10*)		
	GoT	**%**
No qualification	20	65%
Doctorate	1	3%
Not revealed	2	6%
No idea	1	3%
No answer	7	23%
Total	31	100%

Only 13% (4 out of 31organisations) employed cybersecurity experts to control and manage the security and safety of the entire cyberspace in the government organisations. The majority, 74%, (23 organisations) were unable to employ cybersecurity experts to manage the GoT's organisations regarding cyber-safety. About 13% (4 organisations) responded with 'Other/No Answer' to the question.

The majority (97%) responded to the question about the cybersecurity expert qualifications with the answers 'No qualification', 'Not revealed', 'No idea', and 'No answer'. Only one answer (1) (3%) indicated that one organisation got a cybersecurity expert with a PhD qualification.

One of the participants commented that their organisation is managed from overseas. The participant stated that;

> We have a very safe system in our internet control by the DFAT office in Canberra and our IT is very professional. Apart from home which does not have that system or maybe our mobile phone, we are then exposed at our own cost', according to the participant's comment.

5.2.14 Brief of victims involved in cyberattacks

The figures mentioned in the table below summarise the total number of victims, age category, gender, and the region where the OS took place.

Table 18: Summary of victims

No of victim	Age	Gender	Region
1	16 – 20 years	1 Female	Tongatapu
7	31 – 40 years	5 Females 2 Males	All from Tongatapu
3	41 – 50 years	3 - All females	2 from Tongatapu 1 from Niuatoputapu
3	51 – 60 years	3 – All males	All from Tongatapu
Summary			
14 **Total victims**		**9 Females** **5 Males**	**13 from Tongatapu** **1 from Niuatoputapu**

Table 18 shows that:

- The highest portion (9 out of 14 participants) of the victims were females, and 5 victims were males.
- Most of the victims (13 victims) involved in cyberattacks took place in Tongatapu and only 1 victim from Niuatoputapu.
- It is noted that the ages between 31 – 40 years were the most ages involved in cyberattacks.
- The category of the ages between 31 – 40 years is also noted that 5 females out of 7 victims were captured in cyberattacks.
- Three (3) females in the age category of 41 – 50 years were captured in cyberattacks.

- Three (3) males were caught in cyberattacks in the category of 51 – 60 years.
- One female from Tongatapu, the main island in Tonga, in the age category of 16 – 20 years stepped forward to report a cybercriminal case that happened to their extended family.

5.2.15 Cybersecurity Analysis Summary

Niuatoputapu is the smallest region in Tonga and the ICT development is remotely controlled by ISP providers from Tongatapu the main capital of Tonga. The majority, 92%, (13 victims) of OS took place in Tongatapu, the center of ICT. The cybersecurity case that happened in Niuatoputapu is concerning compared to other regions (Vava‘u, Ha‘apai, and ‘Eua).

The effective methods used by scammers to victimise Tongans are:

- email contacts sent from unknown senders,
- email contacts sent via victims’ friends,
- links sent from friends to click and open,
- texts through mobile devices,
- and phone calls from unknown individuals.

With these communication methods, the scammers asked the TIs to provide the following credentials:

- *Bank Information*: account number, username, password, credit card and so on.
- *Personal details*: name, address, DOB, IRD number, security number and so on.
- *Survey*: asked to answer questions in a survey, open an attachment in an email, and click a website link.
- *Friends/Relatives*: asked to give the names of people, friends, relatives, family members, etc.

All the answers from the survey participants who lost money to scammers in Section 5.2.4 and those who lost secret information to scammers in Section 5.2.8 and also shown in *Appendix 3* and *Appendix 4* were collected and classified to each category that they belonged to, to form a thematic analysis. The thematic analysis process and details are shown in *Table 19.* The following sections are the reasons for the participants who were victimised by scammers.

1) Lack of ICT knowledge: There are many quotes related to this point. In this section, two quotes are provided to confirm the lack of ICT knowledge in Tonga. One, is involvement of a 13-year student in an OS case where the girl admitted that: "I did not know enough about online scamming". Two is a comment made by another participant who said:

> '*Oku ou 'ilo leva 'oku 'iai 'a e fa'ahinga ngāue kākā pehee 'aia na'e 'ikai ke 'ilo ki ai. Ko ia ai, kuo 'ilo'i leva 'a e ngāue kākā ni pea u toe tokangaange ke solova mo ta'ofi ha ni'ihi me i he to 'i he ngaahi ngāue kākā ni*. [translation by author] I know now there are such online fraudulent acts that I did not know about before. Now, I know this type of fraudulent activity, and have been more aware to solve and stop others that may be caught by these acts.

2) Greed: TIs were caught by attractive baits (money and luxury items) lured by cyberattacks with empty promises to pay back huge amounts of money or delivered items when pre-payments were received. In the end, there were no items or money were delivered although the victims look forward to receiving the items/money. There is strong wish to gain the desired item. Due to strong desire and lack of ICT knowledge, there was no chance to double-check for the integrity and reality of the advertised product and money before and move on to make the payments. One participant quoted:

> '*Ne u ongo'i manumanu he faka'ali mai e pale 'e ma'u, ka na'aku 'osi 'ilo'i pe ko 'enau ngaue kaka, na'a mole 'eku saving he pangike ha'anau 'ilo 'e ku account numbers*. [translation by author] I felt greedy for the winning prize, but I already knew about this as a scam that I may lose my savings in the bank if they knew my account numbers.

3) Romantic, Love and Empathy: A form of luring the bait and changing the mindset from money to a romantic relationship. A smart tactic used by scammers to connect with victims in different ways but in the end, it is all about OS and cyberattacks. One Tongan innocent internet user (IIU) quoted: "I like the person, and the person kept sending me romantic emails and songs, that's good enough for me to trust that person that I have no idea who he was."

An extreme feeling of deep fondness for the emotional stories sent through emails seeking assistance. With willingness to assist, the emotional stories provided by cyberattacks encourage the victims to pay money. One victim quotes: "I was so emotional when they told me their sad stories', as according to one victim who lost money."

4) Unwillingness to report: An answer from one of the victims is highlighted as; "**Thought to just leave it as it is as there were some other people involved."** The victim, a civil member, denied reporting the case to the MoP and high authority as the victim knows there are other people who got involved in this case of losing money TOP $100 – TOP $1,000 in 1990 - 1999. The case was not clearly explained of how the victim lost money to cyberattacks but it clearly described the unwillingness of the victim to report the case as a fear of the involvement of other people.

5) Lack of cybersecurity training: Most participants, 61%, (73 people/out of 119 participants) did not attempt any workshop or cybersecurity training. In the island of Niuatoputapu (NTT), there were 8 participants who partook in this survey. None of them attended any workshop or cybersecurity training. One victim from NTT was victimised and lost money. This result can be partly related to the lack of training. One of the participants response is shown in the text below.

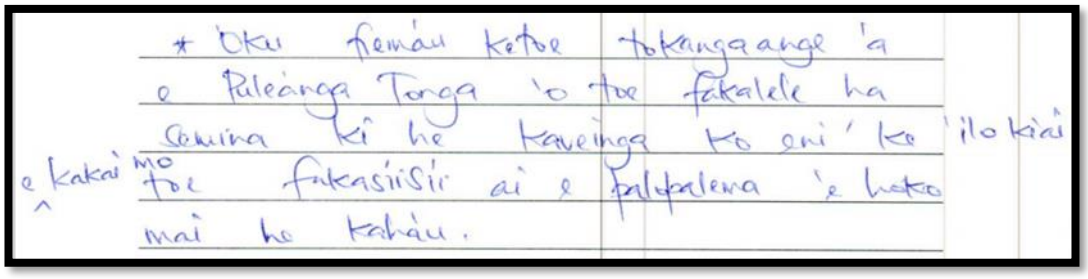


Figure 34: Request from a participant to run a serminar

Figure 34 shows a written message from one of the participants to the GoT.

'Oku fiema'u ke toe tokangaange 'a e Pule'anga Tonga 'o to e fakalele ha ngaahi seminā ki he kaveinga ko 'eni, ke 'ilo ki ai e kakai mo to e fakasi'isi'i ai e palopalema 'e hoko mai he kaha'u. [translation by author] The GoT needs to re-focus on running seminars on this subject, to get people to understand and to minimise future problem.

Another civil servant from one of the government ministries commented that: “ICT division should set up a strong password for each staff member and conduct workshops to familiarize everyone about these issues and ways they can protect them from scammers and losing money.”

Table 19 summarises and classifies the number of answers from the participants (n = 44) explaining the reasons that are related to the loss and almost loss of the credential information including money, to cyberattackers.

Table 19: Thematic Analysis Summary

Types of Attack	Number of Attack
Greed	30
Romantic/love/empathy	6
Lack of cybersecurity training	4
Lack of ICT knowledge	3
Unwillingness to report to authorities	1
Total	**44**

One Tongan Innocent (TI) received a scam email asking for money. The TI looked forward to paying the money, but due to no money afforded during this time, the participant was unable to pay the money. This is the comment from the participant to show disappointment, for not being able to pay the money. “*Na‘aku feinga pe ke ma‘u ha seniti ke ‘ave ka na‘e ‘ikai ma‘u. Na‘aku loto mamahi he ‘ikai ma’u ha sēniti ke ‘ave...* [translation by author] I was trying to get money to send but no money during this time. I was disappointed that I did not have money to send…. ‘.

The thematic analysis identifies the main weaknesses of Tongan Innocents to lure bait delivered by cyberattacks.

5.3 General Cybersecurity Analysis

This section consists of nine questions. It focuses on other dimensions of cybersecurity in Tonga. A short section and it is focused on cyber resilience, isolation/ location, insider threat, cybersecurity knowledge, home-based internet users, cyberbullies, and cyber-grooming.

5.3.1 Other perspective of Cybersecurity in Tonga

Information about the above-mentioned areas were sourced in eight different questions as displayed on *Table 20* below.

A total number of 119 participants from the GoT and People (n = 119). The highest portion for each answer is highlighted in red. Details of the answers are shown in the table below.

Table 20: Tongan perspectives on cybersecurity

Question 1: Isolation of Tonga from outside nations and internal isolation within Tonga (like Haʻapai and Ongo Niua) is a major issue for ICT development.			
Agree	**Unsure**	**Disagree**	**No Answer**
53% 63 participants	29% 34 participants	13% 16 participants	5% 6 participants
Question 2: Do you think the location and exposure of Tonga to hurricanes and cyclones hinder the growth of ICT development?			
Agree	**Unsure**	**Disagree**	**No Answer**
50% 60 participants	20% 24 participants	27% 31 participants	3% 4 participants
Question 3: Cyber resilience helps a lot to speed up ICT recovery after Cyclone Gita destructed Tonga.			
Agree	**Unsure**	**Disagree**	**No Answer**
62% 73 participants	28% 34 participants	7% 8 participants	3% 4 participants
Question 4: Judges in Tonga require to understand cybersecurity knowledge to assist in judging cybercriminals.			
Agree	**Unsure**	**Disagree**	**No Answer**
81% 97 participants	10% 12 participants	5% 5 participants	4% 5 participants
Question 5: Insider threat already exists within some organisations in Tonga			
Agree	**Unsure**	**Disagree**	**No Answer**
66% 79 participants	27% 32 participants	4% 4 participants	3% 4 participants
Question 6: Home Based Internet Users are more likely to victimise by online scammers due to the absence of other supports and limited knowledge of ICT.			

Agree	Unsure	Disagree	No Answer
80% 95 participants	10% 12 participants	6% 7 participants	4% 5 participants
Question 7: Do you think that cyberbullies exist in Tonga now?			
Agree	**Unsure**	**Disagree**	**No Answer**
86% 102 participants	5% 6 participants	3% 4 participants	6% 7 participants
Question 8: Cyber-grooming is about building an emotional relationship with a child to gain trust aiming for exploitation or sexual abuse. Does cyber-grooming exist in Tonga?			
Agree	**Unsure**	**Disagree**	**No Answer**
67% 80 participants	27% 32 participants	4% 5 participants	2% 2 participants

5.3.2 Summary of General Cybersecurity in Tonga

One of the highlights of this section is the judging of cybercriminals in Tonga. Judges require to understand cybersecurity knowledge to assist in judging cybercriminals. Majority of the participants, about 81% (97 participants) agreed with this idea that Tonga's judges need cybersecurity knowledge in their work.

Another area discovered is the existence of cyber-grooming in Tonga. The majority, 67%, (80 participants) agreed that cyber-grooming has already existed in Tonga. Some of the participants made quotations to clarify issues relate to cyber-grooming and cyberbully.

Listed below are comments from the participants regarding questions in *Table 20*.

- Cyber grooming and all those things mentioned happen in Tonga. It is a bad issue. Before I thought that only bad things happen overseas but honestly, today things we watch in movies are happening right near us. I hear a few cases of such things as that and even some silly girls falling for phone calls having sweet voices. And it is not only from strangers but perhaps from someone you may have known but they use false ID.
- Cyber Bullying in Tonga has been raised for the past years, as our people get involved in using technology to perform unnecessary actions over the Internet. ICT in Tonga has benefited our children, young

youths, but at the same time ICT can put our young people at risk of violence, exploitation, and abuse. Threats and lots of other cyberbullies surfaced in our Kingdom when people with less knowledge of securities used media networks to act as parasites and fake profiles on any social media network to attack victims. Therefore, I strongly agree, we need to be trained and well equipped for any harmful issues along the way. Our children are victims of cyberbullying and can affect communities.

- In my own opinion, the major issues for ICT development in Tonga are wrong, people are in control of Government ICT Strategies and Budget, and Government ICT personnel are not working together.
- Cyberbullying, grooming, and all other threats can be witnessed on social media. Need some strong Social Media policy and regulations.

5.4 Cybersecurity Management Analysis

This chapter focuses on basic technical cybersecurity features to maintain a cyber-safe environment in the government ministries. Overall, twelve questions focused on: password, antivirus, cloud computing, updated software, penetration testing, data encryption, data backup, multi-factor authentication, firewall, cyber insurance, business continuity plan, and budget.

5.4.1 Management of cybersecurity

Table 21 summarises the responses from the GoT's organisations (n = 31). Participants were asked to circle the right answers (Yes or No). Some of the participants preferred to provide no answer to the question due to organisations' privacy and restrictions. The highest portions (in both percent (%) and the number of participants) of the answers in the table are highlighted in red colours. Here are the details of the answers given by the participants.

Table 21: More Cybersecurity Questions

Questions	Yes (%)	No (%)	No Answer / Other (%)
Did you/your organisation set up strong password (e.g., combination numbers, letters, symbols (@, #, $, %, ~, & *), both uppercase and lowercase, and at	87% 27 organisations	7% 2 organisations	6% 2 organisations

least six characters) on your computer system			
Did you/your organisation install antivirus software to protect from virus and malicious programs?	84% 26 organisations	10% 3 organisations	6% 2 organisations
Did you/your organisation update software and your computer to the latest version?	71% 22 organisations	23% 7 organisations	6% 2 organisations
Did you/your organisation back up your data regularly?	77% 24 organisations	13% 4 organisations	10% 3 organisations
Did you/your organisation use Cloud Computing Technology to store your data/information?	45% 14 organisations	45% 14 organisations	10% 3 organisations
Did you/your organisation use a firewall to protect your computer system?	80% 25 organisations	10% 3 organisations	10% 3 organisations
Did you/your organisation use multi-factor authentication to access your data/information?	45% 14 organisations	45% 14 organisations	10% 3 organisations
Did you/your organisation use Data Encryption to secure your sensitive information/data?	52% 16 organisations	35% 11 organisations	13% 4 organisations
Did you/your organisation carry out Penetration Testing to test for loopholes on your websites?	19% 6 organisations	65% 20 organisations	16% 5 organisations
Did you/your organisation deploy Cyber insurance to protect your information and cover loss in time of physical/natural disaster?	16% 5 organisations	71% 22 organisations	13% 4 organisations
Did you/your organisation deploy any Business Continuity Plan OR Incident Management Communication Plan?	32% 10 organisations	52% 16 organisations	16% 5 organisations
Did you/your organisation provide sufficient fund (budget) to purchase updated antivirus and latest software version?	48% 15 organisations	39% 12 organisations	13% 4 organisations

5.4.2 Summary of Section 5.4

Based on minority answers in *Table 21*, five key areas required to focus grounded on the results collected from the survey participants are: Cloud computing; Penetration testing; Multi-factor authentication; Cyber insurance; Business Continuity Plan OR Incident Management Communication Plan.

As the components of these abovementioned areas were still in the minority category, there are needs to deploy more of these five cybersecurity components to reach maximum protection level or to maintain a cyber-safe environment in Tonga. Details of the findings in these areas are listed below:

- Only 45% (14 organisations) deployed Cloud Computing technology to store their data/information.
- About 65% (20 organisations) did not carry out the Penetration Testing process to check vulnerabilities and loopholes of websites and computer systems.
- Only 45% (14 organisations) adopted multi-factor authentication to access their data/information.
- Only 16% (5 organisations) implemented cyber insurance to protect information and cover loss in a time of physical/natural disaster.
- Only 32% (10 organisations) deployed Business Continuity Plan OR Incident Management Communication Plan.

The information provided below summarises the participants' comments/quotes and personal assessments about cybersecurity in Tonga based on the questions in *Table 21*. Details are listed below:

- Our organisation is far too late to use them. (This comment was from one of the government's senior officials who is currently working on an outer island. 'Far too late to use' means for the use of a secured password character, antivirus, cloud computing, updated software, penetration testing, data encryption, data backup, multi-factor authentication, firewall, cyber insurance, business continuity plan, and budget).
- No expert to recommend those security features to Management. Perhaps just ignorance of risk at stake in terms of intelligence information.

- Either there is no expertise available within the organisation or not enough funds to carry out these tasks.
- Lack of skilled staff in the area of cybercrime.
- We are not yet using cloud computing technology, but we are planning to use a cloud VM for our system as a backup infrastructure and data.
- We are not using multi-factor authentication, no penetration testing, no cyber-insurance, and no cybersecurity expert to check overall safety BUT we hope in the future we have to implement those, some are depending on the IT budget, and some we don't have the resources and the capacity. Also, we need more training to gain some knowledge and have more experience.

5.5 Cybersecurity Preventions Analysis

This chapter addresses some prevention features based on technical and non-technical attributes. The main contents of the questions are defensive and prevention tactics. Target participants were from GoT's organisations and representative of the people (n = 119).

5.5.1 Preventative Aspects

The highest portions (in both percent (%) and the number of participants) of the answers in the table are highlighted in red colours. Details of the answers are summarised in *Table 22*.

Table 22: Preventative Questions

Question 1: To Conduct more cybersecurity workshops could assist to reduce Online Scamming.			
Agree	**Unsure**	**Disagree**	**No Answer**
95% 114 participants	1% 1 participant	1% 1 participant	3% 3 participants
Question 2: Training and updating the IT knowledge of Tongan people assists in reducing Online Scamming.			
Agree	**Unsure**	**Disagree**	**No Answer**
97% 115 participants	0% participants	1% 1 participant	2% 3 participants

Question 3: Sending students overseas for further studies on cybersecurity will bring new knowledge to assist Tonga.			
Agree	**Unsure**	**Disagree**	**No Answer**
96% 114 participants	0% 0 participant	1% 1 participant	3% 4 participants
Question 4: Government of Tonga is to consider planning to include some basic training on cybersecurity in the Government Secondary School level.			
Agree	**Unsure**	**Disagree**	**No Answer**
94% 111 participants	3% 4 participants	0% 0 participants	3% 4 participants
Question 5: To hire Cyber Security Experts will assist Tonga to identify security vulnerabilities.			
Agree	**Unsure**	**Disagree**	**No Answer**
93% 111 participants	2% 2 participants	2% 3 participants	3% 3 participants
Question 6: People of Tonga together with the Government ministries and organisations could work together to fight against Online Scamming.			
Agree	**Unsure**	**Disagree**	**No Answer**
97% 115 participants	1% 1 participant	0% 0 participants	2% 3 participants
Question 7: Do not reply to any email sent to you from an unknown sender or someone you do not know.			
Agree	**Unsure**	**Disagree**	**No Answer**
93% 110 participants	2% 3 participants	3% 3 participants	2% 3 participants
Question 8: Open an email from an unknown sender confirms your email address is alive, open an opportunity for the senders to respond back, and make further offers.			
Agree	**Unsure**	**Disagree**	**No Answer**
82% 97 participants	6% 7 participants	9% 11 participants	3% 4 participants
Question 9: If you are suspicious of any contact, it is safer to do further search about the contacted senders.			
Agree	**Unsure**	**Disagree**	**No Answer**
92% 109 participants	2% 2 participants	4% 5 participants	2% 3 participants

Question 10: If you are suspicious of websites, it is good to seek assistance from other people including IT experts.			
Agree	**Unsure**	**Disagree**	**No Answer**
92% 108 participants	3% 4 participants	3% 4 participants	2% 3 participants
Question 11: Security Policy, management, and other Policies are effective tools to be deployed.			
Agree	**Unsure**	**Disagree**	**No Answer**
91% 108 participants	5% 6 participants	1% 1 participant	3% 4 participants

5.5.2 Summary of Cybersecurity Prevention

Most participants agreed with the 11 questions asked. However, there are significant areas to be considered as listed below.

- *Overseas Training*: About 96% (114 participants) agreed with the idea of sending students overseas for further studies on cybersecurity and bringing new knowledge to assist Tonga.
- *School syllabus*: The majority, 94%, (111 participants) agreed with the idea of including some basic cybersecurity training in the Government Secondary Schools' curriculum.
- *Expert*: About 93% (111 participants) agreed with the idea to hire Cyber Security Experts to assist in identifying cybersecurity vulnerabilities on the entire ICT systems.
- *Teamwork*: About 97% (115 participants) agreed with the idea that people together with the Government ministries could work together to fight against online scamming.
- *Security Policy*: Majority, 91%, (108 participants) agreed to deploy cybersecurity policy, management policy, and other policies for the confidentiality, integrity, and availability of systems and information.

5.5.3 Cyber Resilience

The cyber resilience section is summarised in Section 3.4.2 of the Literature Review. In February 2018, Tongatapu, the main island of Tonga, was struck by cyclone Gita, affecting thousands of people. Internal and external communication

was broken down. Overseas contact, to check for family wellbeing, was a major issue due to the breakdown of telecommunication facilities. There was a question to the survey participants (the GoT and People (n = 119)) asked about the process of cyber resilience that helps to speed up ICT recovery after the destruction caused by this category five cyclone.

According to answers provided, the majority, 62%, (73 participants) agreed with the idea of cyber resilience as the process of ICT speed recovery. About 31% (38 participants) were doubted and not able to answer this question. The minority, 7%, (8 participants) disagreed with the idea of cyber resilience as the process of speed recovery after the category five cyclone Gita destroyed Tonga's ICT in 2018.

5.6 Culture Analysis

The Tongan culture section is summarised in Section 2.10. Cultural Analysis based on participants (n = 15) who were knowledgeable and experienced in Tongan culture. Participants were thoroughly selected from former/existing primary/secondary/tertiary teachers, church, psychology, bank, airline, insurance, and pensioner. Besides, other participants were selected from overseas as it is essential to compare their views with the local citizens. All the participants gained academic backgrounds ranging from Diplomas up to Doctorate degrees.

Tongan values are also known as Golden Pillars; respect, humility, nurturing the relationship, love, and loyalty. The Golden Pillars and Tongan concepts were combined in the final part of the questionnaire. This combination intends to investigate the influences in controlling or possibly act as a catalyst to speed up the spreading of online scamming (OS) in Tonga. This means the focus is viewed from two sides – Tongans as victims or as perpetrators of OS.

Here are the main components (listed below) of the Golden Pillars and Tongan concepts that deployed in the final section of the questionnaire:

- *Kavei Koula 'a e Tonga* (Tongan Golden Values)
- *Tala ke i Kapa na'a ke too ki Mala* ('Tell it while still in Kapa')
- *Tahi Kulokula* (Sea of Red)
- *Mate ma'a Tonga* (Die for Tonga)
- *Mate pē Tonga he ngaue 'a e Tonga* (Tongan-kills-Tongan)

- *Tui Faka-Kalisitiane pe Tui Faka-Lotu* (Religious belief)
- *Fakatu'utu'unga e nofo* (Hierarchal Rank)
- *Lea Faka-Tonga* (Tongan Language)

5.6.1 Tongan Golden Pillars (Kavei Koula 'a e Tonga)

Tongan Golden Pillars are the golden core values of Tongan culture. Golden Pillars are *faka'apa'apa* (respect), *lototō* (humility), *tauhi-vā* (nurturing relationship), *'ofa* (love), and *mamahi'ime'a* (loyalty or sense of responsibility).

As mentioned previously, this section provides two views. Firstly, Tongans as victims of OS, and secondly, Tongans as perpetrators. Some subdivisions provide two views while others focus on one view. Here are the types of questions that are set out in the questionnaires to interview the survey participants.

A question asked (see Question 19 in *Appendix 12*): *Are you going to report the scammer within the Tongan community to the police/ to the supervisor/ town officer etc. or you keep it secret and remain silent?* The answer to this question is summarised in *Figure 35*, below.

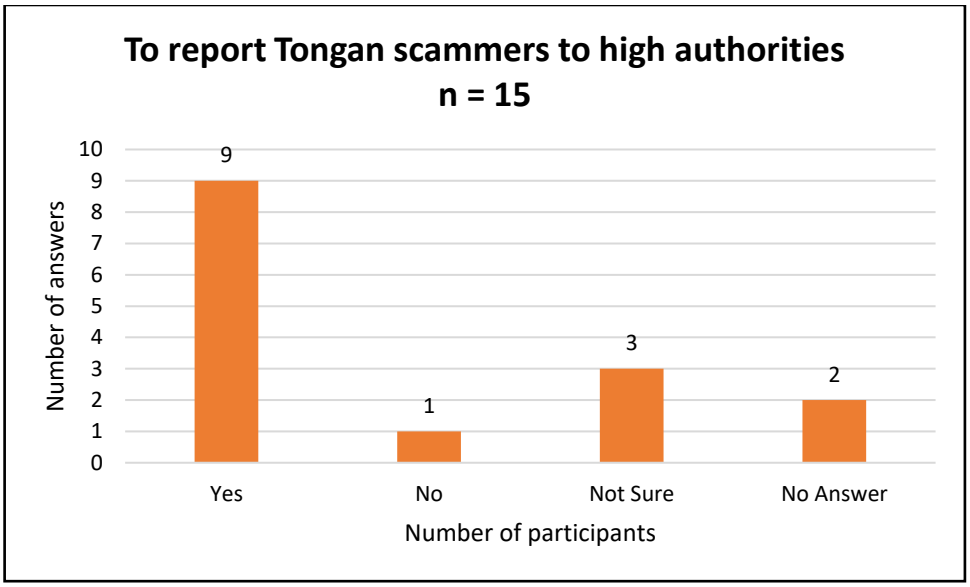


Figure 35: To report scammers to authorities

Figure 35 refers to the responses and answers from the participants. The majority, 60%, (9 participants) believed that any online scamming case that happens within Tongan communities, no matter close friends or close relatives, must be referred to the MoP and higher authorities. The remaining portions refer their answers to 'Not

Sure', 20%, (3 participants); 'Other/No Answer', 13%, (2 participants); and 'No" (7%) (1 participant).

The one participant that answered 'No' to the question informed the reason for not agree to refer to the MoP and authories is;

> Koe'uhi ko hoku kāinga pē maheni, te u feinga leva keu 'uluaki talanoa kiate ia fakafo'ituitui pē pea 'oanga ha akonaki kiate ia kihe me'a 'oku ne fai 'oku 'ikai sai. Pea koeha ha'ane tali pe respond ki he'ema talanoa pea mei ai leva ki he sitepu hoko, koe talanoa kiha taha tokoni pē counsellor ke fai ha ngāue ki ai. Pea ke hoko atu ai pe 'ene faihala pea fakahoko leva ki 'api polisi. Ka kiate au, fiema'u keu 'ulutaki talanoa moia. [translation by author] Because the scammer is my family and friend, I will attempt to take personal discussion and give precautionary advice, and informed that the work carried out is not good. Whatever the answer from the scammer then we move to the next step, to seek an advise from the counselor to take action. If the scammer continues doing the same action of scamming then the next step is to refer to the MoP. For me, I need to first discuss the case with the scammer.

A similar type of question asked (see Question 22 in *Appendix 12*): *What about if this person is the leader of the village, noble, church leader, Government leader, or leading officials? What are you going to do*? *Do you still insist on reporting them to the authorities and police*? The answer for this question is summarised in the bar graph below in *Figure 36*.

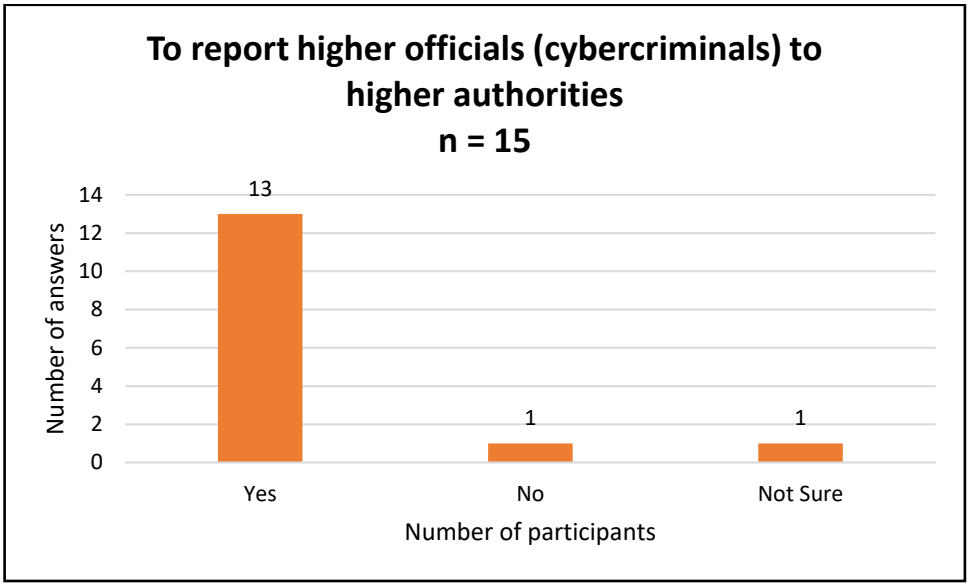


Figure 36: Report to higher authorities

The majority 87% (13 participants) agreed, to report any online scamming case to higher authorities no matter the respected position or higher rank in the Tongan community. However, one (1) participant (6%) choose the answer 'No, which means that the participant denied reporting to the MoP or higher authorities. The participant's answer is shown in *Figure 37*.

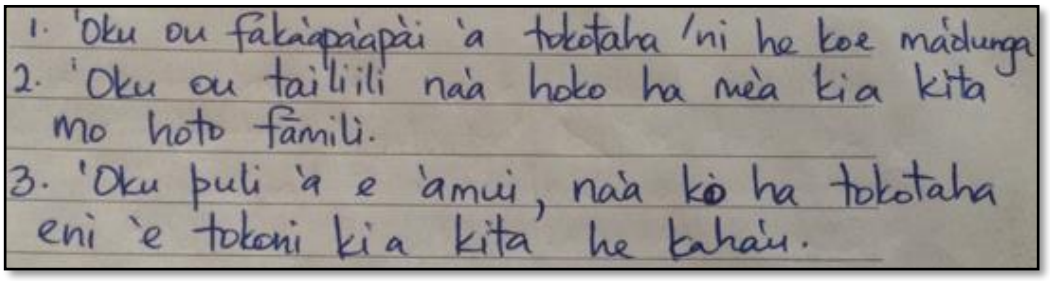


Figure 37: Reasons for not reporting to related authorities

Here are the English translations for the reasons for not reporting the scammers as shown in the answers above:

1. '*Oku ou faka'apa'apa'i 'a e tokotaha ni he ko e ma'olunga.* I am respecting this person (scammer) due to his high position.
2. '*Oku ou tailiili na'a hoko ha me'a ki a kita mo hoto famili*. I am scared if something happens to myself and my family.

3. ’*Oku puli ‘a e ‘amui, na‘a ko ha tokotaha ‘eni ‘e tokoni ki a kita he kaha‘u*. The future is unknown, who knows this person (scammer) I am going to report will assist me in the future.

5.6.2 Summary of Cultural Analysis

According to the information and answers collected from the participants, the core values of Tongan, hierarchal rank, and other cultural factors can affect the process of trying to control cyberattacks and OS in Tonga. Most of the participants (60% (9 participants)) agreed to report any cybercriminal case to higher authorities and MoP. Similar views agreed by the majority, 87%, (13 participants) to report higher position people such as village leader, noble, church leader, Government leader, or leading officials within the Tongan community to higher authorities.

The opposition from one participant is alerted as the antagonism-ideas supported Tongan values and cultures. To summarise the antagonism-response from the participant in *Figure 37*, here are the main areas that were emphasised:

1. *Respect* – the judgment is not based on the illegal and fraudulent acts performed by the scammer, but the decision is based on cultural respect (*faka‘apa‘apa*) to the scammers.
2. *Hierarchal rank* – similar situation of judgment based on respect as mentioned above. The judgment is now based on hierarchal rank or higher position in the society. One participant stated that; I am respecting this person (scammer) because of his high position. ‘*Oku ou faka‘apa‘apa‘i ‘a e tokotaha ni koe‘uhi ko e ma‘olunga*.
3. *Fear* – a sense of terror, if the case is reported there is an unsecured feeling of what happens in the future. “I am scared if something happens to my family and myself” (‘*Oku ou tailiili na‘a hoko ha me‘a ki a kita mo hoto famili*).
4. *Environmental instability* – the feeling of fear grounded on the environmental surroundings. For example, the fear of losing jobs, the presence and enforcement of the law to secure the participants from physical attacks, family and community pressure, and feeling of isolation.
5. *A wheel of fortune* – an outlook or view of the future, a chance of allowing elements of changes, and “whatever goes around comes around”. “The future is unknown, who knows this person (scammer) I am going to report will assist

> me in the future" (‘*Oku puli ‘a e ‘amui, na’a ko ha tokotaha ‘e ni ‘e tokoni ki a kita he kaha‘u*) according to the participant's comments. The participant doesn't want the same thing to happen to their family, to report someone's failure as there is a strong belief that someone will do the similar thing of reporting to the higher authorities.

One participant provided two contradicting answers. The first answer relates to reporting of a scammer. If the scammer is a friend or close family, the action of reporting to higher authorities and MoP is not conducted. The scammer was approach and advice were given to consult to a counselor. The first opportunity is offered by the participant because the scammer is a close friend and relative. On the other hand, the same participant gave a brief answer that if the scammer is not a friend or relative, the case must consult related authorities and MoP. There is no chance given as the scammer is not a close friend or relative.

A verbal discussion with the same participant about the two contradicted answers (mentioned above) to clarify as nonsenses and immorals to report one and denied the other of doing the similar cybercrime. The answer presented by the participant that the judgment was based on Tongan cultural values or Tongan Golden Pillars; respect (faka‘apa‘apa), humility (lototō), nurturing relationship (tauhi-vā) love (‘ofa), and loyalty or sense of responsibility (mamahi‘ime‘a).

Here is the answer from the participant:

> *Kapau ko e tokotaha ‘oku ‘ikai tema maheni, te u fakahoko leva ia ki ‘api polisi ke fai ‘e he Pule‘anga e ngāue ki ai, he ‘oku ‘ikai te u ‘ilo pe ko e tokotaha natula fēfē ia. ‘I he taimi tatau ‘oku ou faka‘amu ke u talanoa mo ia, ka koe‘uhi ‘oku ‘ikai tema maheni pea ‘oku ‘ikai te u loto ke u kaunoa‘ia ka e ‘ave pe kihe feitu‘u totonu ke fai ha‘anau ngāue ki ai*. [translation by author] If the scammer is not my friend, I will report it to the MoP to act upon him, because I do not know the nature of this person. At the same time, I need to meet and discuss with the scammer. Because I am not a friend of the scammer and am reluctant to interfere but to take to the right place to work on this person.

Another participant stepped forward to show similar answer for the reason of denial to report to the police:

> *He ʻikai te u lipooti ʻe au. Naʻa ʻoku ʻi ai ha ʻuhinga ʻo e faihia ʻa e tokotaha ko ia ka te kaunoa atu kita. Takitaha nofo pē ʻo tokangaʻi kita*. [translation by author] I am not going to report the scammer. It might be a reason for this person to attempt the scam, but I am interfered of this action. Stay in your own and look after yourself.

5.6.3 Tongan Proverb

"*Tala ke i Kapa naʻa ke tō ki Mala"* ("Tell it while still in Kapa") is a Tongan proverb. The metaphoric theme behind this proverb is for the people of Tonga to prepare for problems in the future. At whatever time the problems arrive, preparations are already in place and Tongans can know the right actions to do. The concept of this proverb is a warning for Tonga to be ready for the influences of ICT technology and to be aware of the emerging cybercrimes in the Kingdom (see Section 2.2).

The first question asked (see Question 15 in *Appendix 12*): *Do you think the main idea of 'Tala ke i Kapa naʻa ke tō ki Mala'* (to give precautionary advice to be aware of danger ahead) *can be applied in this study and will assist in trying to control online scamming in Tonga*?

Table 23: Agreed with Tongan Proverb

Strongly Agree	Agree	Unsure	Disagree	Strongly disgree
87% 13 participants	13% 2 participants	0%	0%	0%

Table 23 represents the answers from the participants. About 100% (15 participants) agreed with the concept of the Tongan Proverb *'Tala ke i Kapa naʻa ke tō ki Mala'* ("Tell it while still in Kapa") to be applied as a precautionary warning for Tongan citizens about the impacts of ICT.

To clarify more about *'Tala ke i Kapa naʻa ke tō ki Mala'*, another open question asked to write and explain the reason for their choices. *Please explain your reason compared to your choice above*?

Here are two answers (Tongan language) from two participants provided below in response to this question. One of the participants said;

> *‘Oku mahu‘inga ke ‘omai e ngaahi* concept*/fakakaukau/‘ilo faka-Tonga ke tokoni ki hono fakafepaki‘i ‘aki e ngaahi palopalema ‘oku hanganaki ke ‘ohofi hotau kāinga Tonga/. Pea ‘oku lelei ‘a e palovepi/ ni he ‘oku/ ne ‘omai e naunau ‘o e tokateu pea tekemui mai ai e* values *pē ‘ulungaanga fakafonua kae malava ke tautonu e fakafepaki ‘oku fakahoko.* [translation by author] It is essential to bring some of the Tongan concepts/ideas/knowledge to assist in fighting against the problems that likely to attack Tongan people in the future. Also, this proverb brings the elementary precaution, values, and Tongan culture to resist the existing cyberattacks.
>
> The other stated that:
>
> *‘Oku matu’aki mahu‘inga ketau faka‘ehi‘ehi telia na‘a tau tō ki ha fakatamaki. ‘E ma‘ama‘a ange ‘etau faka‘ehi‘ehi mei ha palopalema ‘i ha‘atau tō ki he palopalema pea tau toki feinga ke solova.* [translation by author] An essential element is to prevent before fail into danger. It is easier to prevent us from the problem rather than falling into the issue and trying to solve it.

5.6.4 Sea of Red (SoR) (Tahi Kulokula)

The Sea of Red section is discussed in Section 2.10. The philosophy behind SoR (when Tongan people are dressed in Red clothes) does not only represent Tongan Golden Pillars (*faka‘apa‘apa*, *lototō*), *tauhi-vā*, *‘ofa*, and *mamahi‘ime‘a*) but also symbolises unity and solidarity of the people of Tonga. In recent years, people were dressed in red to show their respect for the Tongan-related overseas players in league and rugby who are willing to represent Tonga. The players’ contribution is not only respect to their parents but shows humility, nurturing the relationship, love, and loyalty to the Tongans. Combining the Tongan Golden Pillars with the Sea of Red is a strong defensive approach to defend online scamming.

The SoR demonstrates *loto-taha* (voluntary agreement or ‘of one-mind’) to work together as one people and one nation to fight against internet evildoers. The

atmosphere of SoR signifies unity, solidarity, teamwork, warm heart, and love of Tongans. To transfer the concept of SoR to work in an ICT environment is believed to be a strong defensive mechanism to counteract online scamming in Tonga.

In this context, SoR is referred to the *loto-taha* (voluntary agreement or of one mind) to work together or teamwork. A question asked (see Question 24 in *Appendix 12*): *Do you think the concept of the SoR is applicable to use in trying to control the growth of OS in Tonga*?

To prove the theory of unity, concord, concur, unanimous (*loto-taha*) of the People of Tonga by using the concept of the SoR. There are the responses from the survey participants for this question as mentioned in *Figure 38*.

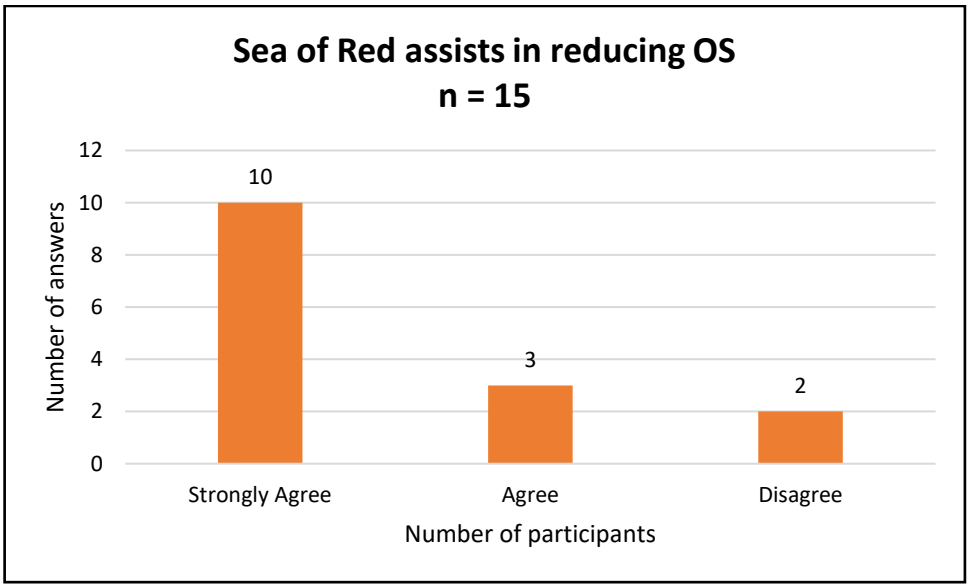


Figure 38: Sea of Red relates to OS

The majority, 67%, (10 participants) chose 'Strongly Agree' and 20%, (3 participants) opted to choose 'Agree'. Therefore, the combination of 'Strongly Agree' + 'Agree' equals to 87% (13 participants). Only 13% (2 participants) disagreed with the concept of SoR.

Another question asked (see Question 25 in *Appendix 12*): *If you agree/strongly agree with the concept of Sea of Red, please explain how this idea will assist in controlling cybercrime in Tonga*?

Here are the responses and suggestions (summarises below) from the people regarding the SoR.

*Fokotu‘u ha ngaahi kulupu/*agen*t meihe ngaahi vahefonua kenau kafataha hono fakataukei‘i e kakai ki he me‘a totonu kenau fai pea nau ngāue fakataha mo e kau ma‘u mafai/polisi/ ki ho no fakatotolo‘i.* [translation by author] establish regional groups/agents to guide people in the proper actions to conduct and to work together with the authorities/police on how to investigate fraudulent acts.

Ke vahevahe atu e ‘ilo ‘o e feinga ako ni ki he ngaahi lotofale, siasi, mo e Pule’anga. [translation by author] To share the result of this research to families, church, and the government.

Vahevahe atu e ‘ilo mo e taukei meihe savea ni ke tokoni ki he kakai ‘o e fonua ni. [translation by author] To share the knowledge and experience from this survey to assist with the people of the land.

Ngaue fakataha ‘a e kau matiketika ‘i he tekinolosia pea, nau oungongataha mo fetokoni‘aki. [translation by author] ICT experts are to work together as one man (*oungongataha*) and help each other.

‘*Ke ngaue fakataha e Pule‘anga, Siasi, ngaahi psisnisi mo e fonuā. Ako‘i ha ngaahi polokalama komupiuta ke ‘ilo ‘e he kakai pea ‘e fakasi‘isi‘i leva ai e hoko e palopalema*. [translation by author] The government, church, businesses, and the nation (Tonga) are to work together. To educate computer programs to be understand by the people as way to reduce the problem.

Fokotu’u ha ngaahi lao ke muimi pau ki ai e kakai e fonua pea hilifaki e tautea ki he kakai ‘oku ni’ihi ‘oku nau fai e ngaahi ngaue pango. [translation by author] To establish laws to be accurately followed by the people of Tonga and to penalise the people that accountable for these illegal acts.

5.6.5 Summary of Sea of Red Analysis

Sea of Red or the *Red Sea* has proved to be a practical method for the GoT, villages, churches, and communities to fight against OS. The overall 100% (15 participants) agreed with the SoR as an appropriate defensive technique for Tongans.

Other suggestions from the participants relate to the SoR and details are listed as:

- To establish regional groups/agents to work together with the authorities/police on how to investigate fraudulent acts.
- A call for the ICT experts to work together as one man (*oungongataha*) and help each other.
- This research result is to share with the people of Tonga.
- All the members of the churches, communities, GoT, businesses, and other organisations are to collaborate and work together as one (*oungongataha*)
- The educational computer programs are to be taught to all the people.

Based on this information, SoR is an appropriate human ICT defensive and awareness tool to be deployed to assist in reducing OS in Tonga.

5.6.6 Mate ma‘a Tonga (MMT) (Die for Tonga)

The *Mate ma‘a Tonga (MMT)* or (*'Die for Tonga*') section is discussed in Section 2.10.3 and Section 2.10.5. The idea of MMT or (‘*Die for Tonga*’) which means love for Tonga. A question asked (see Question 27 in *Appendix 12*): *Do you believe that the idea MMT or (‘Die for Tonga’) assists in managing the growth of the cheating website in Tonga?*

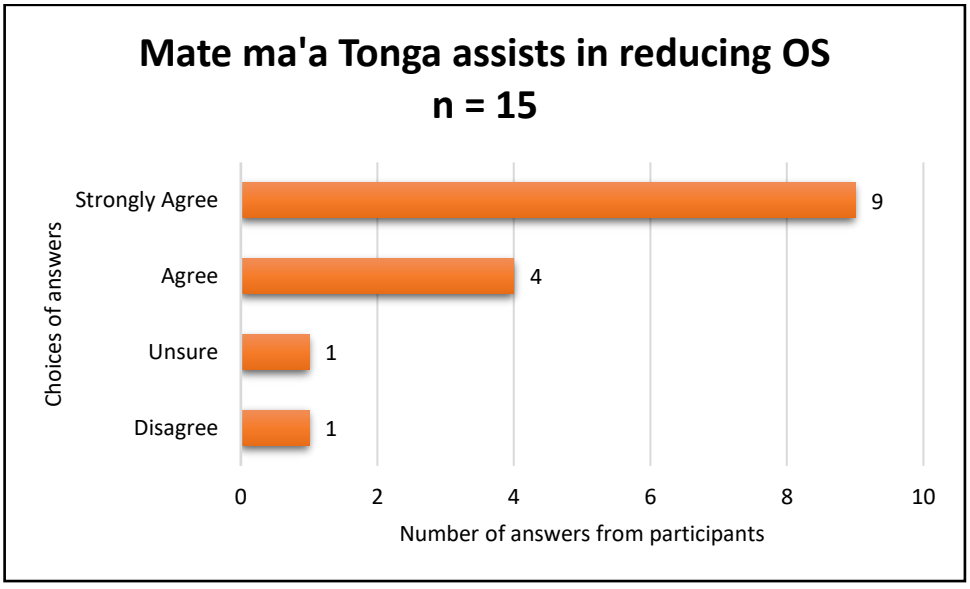


Figure 39: Concept of Mate ma'a Tonga

Figure 39 represents the answer to the MMT question. The majority, 60%, (9 participants) strongly agreed and 27% (4 participants) also agreed with this concept as a defensive mechanism to assist in the process of reducing OS. This means that

87% (13 participants) agreed and supported the idea of MMT to be an awareness and prevention tool for OS. Only 13% (2 participants) did not agree and were unsure with this idea.

Another open question asked the participants to explain how to implement the theory of MMT in relation to OS (see Question 29 in *Appendix 12*). Here are parts of the answers from the participants as written below:

- *Ngaue fakataha mo na u fevahevahe'aki hano trace ha palopalema 'e hoko 'i Tonga ni*. [translation by author] Sharing and working together to trace issue that will happen in Tonga.
- *Mate ma'a Tonga, ko'ete mamahi'i hoto fatongia, 'ofa ai pea faingata'a leva ke ta fa'u ha fa'ahinga ngāue kākā*. [translation by author] MMT is the sense of responsibility. Love our responsibility makes hard to perform illegal acts.
- *Ko hono kumi hakili 'a e kau fai hia, pe koe kau kãkã, 'o faka'ilo pea ta'ofi kei taimi*. [translation by author] Take deep investigation for the cybercriminals or fraudsters and take legal action to stop on time.
- *Ne foaki 'ehe 'Uluaki Fã hotau fonua ki Langi, ko e mate ia ma'a Tonga. Me'a kotoa pē ke fakamu'omu'a 'a e maama faka-'Otua. Ke fai ha lotu hūfia mo ha 'aukai he ngaahi feohi'anga, … ko e tataki 'a e laumālie 'e tonu leva e hala fononga, ko e tonu ia 'eta mate ma'a Tonga*…….. [translation by author] The First Christian King, Siaosi Tupou 1, offered our country, Tonga, to God is exactly what it means *Die for Tonga.* Our priority is to let the light of God lead us …the guidance of the spirit leads to the right pathway of the journey, that what ***Mate ma'a Tonga*** is……. .
- *Ka malohi pē 'ofa fonua mo e 'ofa fakatokoua 'a e Tonga, he'ikai ke lahi e ngaahi ola kovi ngaue'aki 'o e tekinolosia 'i hotau k'i fonua. Te nau fetokoni'aki ke malu'i mo taliteke'i e ngaahi ola kovi 'o e tekinolosia*. [translation by author] An empowerment of love for our land and brotherly love it will reduce cybercriminals in our nation.
- *'Ilo 'e he Tonga ho no Tonga ko e key ia*. [translation by author] The main key is when Tongans know their Tongan as Tongans.

- *Ko e taimi pē ʻoku tau mate ai ki hotau Tonga heʻikai toe mahuʻinga ha meʻa ia. Ko ʻetau mate pē ki he faitotonu mo e melino ko ʻetau liʻaki ia e faihala*. [translation by author] When we prioritise our Tongan identity, there is nothing else that is more important. When we all die for integrity and peace, that is when we eliminate dishonesty.
- ʻ*Oku fiemaʻu ke tau mateakiʻi hotau Tonga ʻaki ʻetau fetokoniʻaki pea ke langa ha Tonga ʻoku lelei maʻa e Tonga*. [translation by author] There are needs our sense of responsibility as Tongans to work together to built Tongans to benefit Tonga.

5.6.7 Summary of MMT Analysis

Like the idea of the *Sea of Red*, the MMT proved to be a practical method for Tonga in fighting against the OS. Although the majority (87%) (13 participants) agreed with the idea of MMT, there are other significant points and suggestions from the participants. The focal suggestions from the participants are:

- The appurtenances, give-back, and the process of ʻ*Tukufonua ki Langi*ʼ (offered our land and people, Tonga, to God) reflects the MMT.
- When we die for Tonga there is nothing more important. When we all die for honesty and peace, we reject dishonesty.
- *Loto-taha* (unity) and *Uouongataha* (solidarity) and are revealed in MMT based on the answers collected from the participants.
- Tongan Golden values are also revealed in MMT.

Based on these suggestions, MMT is an appropriate human ICT defensive and awareness tool to be deployed to assist in reducing OS.

5.6.8 Mate pē Tonga/ he ngāue ʻa e Tonga/ (Tongan-kills-Tongan)

The *Mate pe Tonga he ngaue ʻa e Tonga* section is summarised in Section 2. 10.5. Tongan-kills-Tongan (TkT) is not targeted for a physical attack to kill. A mislead-plan of action to harm individuals or people in the Tongan community. The idea behind this plan is the victims who were victimised by scammers could possibly set up the same procedures to victimise other Tongans, so they (victim vs people) get involved in the same case and remain at the same level.

The participants were asked whether they know anyone in Tongan community who already performed (‘Mate pe Tonga he ngaue ‘a e Tonga (TkT) and that they are trapped in this case? (See Question 31 in *Appendix 12*). The answers are summarised in *Figure 40*. The highest portion, 60%, (9 participants) were not involved and 20% (3 participants) were not sure about the involvement of people in TkT. About 20% (3 participants) were attacked and victmised by cyberattacks using the TkT method.

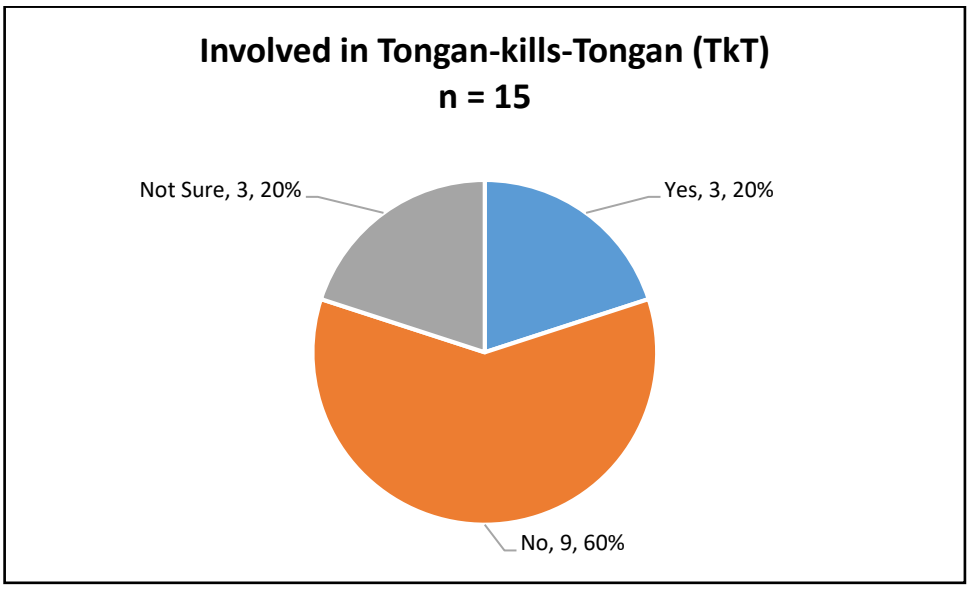


Figure 40: Victims of TkT

The majority, 60%, (9 participants) did not involve in TkT. Only 20% (3 participants) were involved in TkT. The main idea of this question is to search for the existence of TkT in the Tongan community. Therefore, it is evident TkK is existed in Tonga.

Here is the answer from the victimised participant as shown below in *Figure 41*.

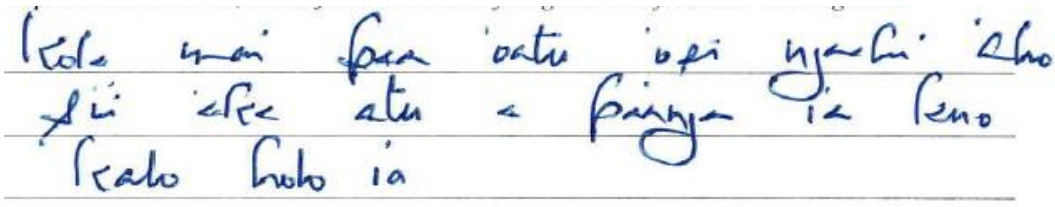


Figure 41: An answer from one victim of TkT

Kole mai pea ʻoatu, ʻosi ngaahi ʻaho siʻi, ʻeke atu e paʻanga ia kuo kalo holo ia. [translation by author] The scammer asked me, I agreed to give. After several days, I asked for my money, but the scammer paid no attention.'

The researcher contacted via Facebook Messenger (FM) with the victim (Monday 12/04/2021), who is a *faifekau* (church minister), to explain more on this case. The *faifekau* replied and wrote in the FM:

> '…..*ko hoku best friend pē i Tonga ni ne haʻu ʻo kole ʻene sēniti ki he'ene kiʻi meʻa faakfamili, peau tokoni ange ʻo ʻave ʻene fiema'u pea mei ai ki he aho ni te'eki pe ha toe felogoaki*. [translation by author] The attacker is my best friend in Tonga. He came and asked me for money for a family occasion and I helped him. And from then to this day I haven't heard from him.

This case is not written in the record of the number of victims who lost money to scammers because it is not related to online scamming. The process of giving money was hand-to-hand, and the person who took the money was a close friend of the victim. Both the victim and the scammer were close friends and knew each other well. However, it is important to mention that the nature of this case is exactly the deployment of TkT for a fraudulent act.

5.6.9 Summary of TkT analysis

Although the minority (3 victims) were involved, victmised, and lost money in this way, there is evidence that the method of TkT has proved to be practiced in the Tongan community. There is a high possibility that TkT will be deployed as a way of face-to-face or online communication between victim and attacker within the Tongan community.

The Religious belief Section 2.11 discussed the power of the words of the *faifekau* (church ministers) or People of God (PoG). As words of church leaders and *faifekau* are very powerful they will assist in delivering messages to the people through church services in the villages and communities to avoid and stop cheating other local Tongans using TkT.

The majority, 83%, (11 participants) agreed and supported that religious beliefs working and that the *faifekau* and religious officials acquire the power to deliver

messages to the people to keep away from cybercrimes. Therefore, the words or messages from the *faifekau* will be a proper remedy for the issue of TkT. This solution is only for cases within Tonga without the inclusion of outsiders from overseas. That is for the local Tongans who propose to use TkT to cheat others within the Tongan community.

5.6.10 Hierarchal Rank (Fakatu‘utu‘unga e nofo)

Section 1.2 summarises the Hierarchal Rank in the Tongan Society. Tongan structural rank is the King at the highest authority, the nobles, and the people or commoners at the bottom. Tongan way of living is unique following hierarchal structure starting at the top beak (King) and breaking down to the bottom (commoners). Commoners are at the lowest level of the hierarchal triad and must adhere to the message from these above as they (King, nobles, etc.) get more power.

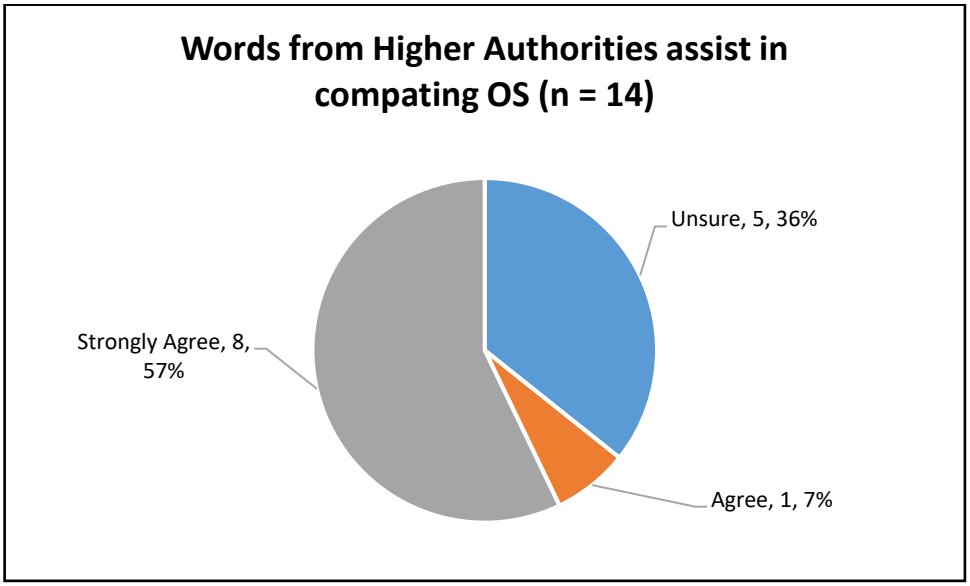


Figure 42: Words of higher authorities

The participants were asked whether any announcement/message is sent from the top of the hierarchal triad (nobles) to the commoners to be aware of cybercrimes and whether they think commoners will accept this message? (See Question 54 in *Appendix 12*)

The responses to this question are summarised in the pie graph shown above. (The number of survey participants is reduced from 15 to 14 as one participant was unable to complete the rest of the survey).

Figure 42 reveals the power of words of higher citizens in the Tongan community. The majority, 64%, (9 participants) agreed to accept announcements/messages from the top of the hierarchal triad (nobles) to the commoners to be aware of cybercrimes. About 36% (5 participants) were unsure of accepting announcements/messages from higher authorities.

Another question asked (see Question 56 in *Appendix 12*): *Do you think it is still important for Tongans to maintain the Tongan hierarchal structure to keep the mutual relationship between commoners and higher rank people*?

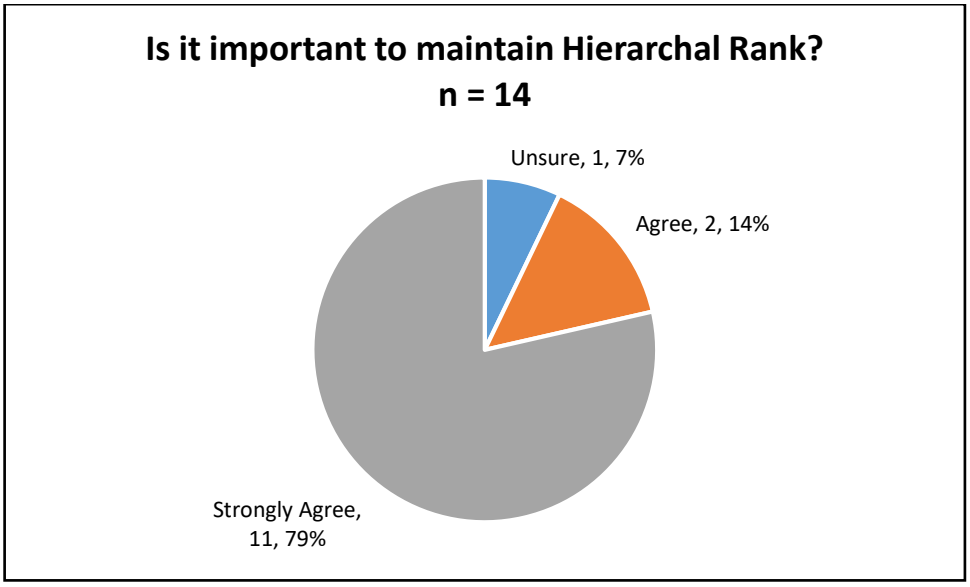


Figure 43: Agree to maintain Hierarchal Rank

Figure 43 represents the answer to maintaining the hierarchal rank. About 93% (13 participants) supported the idea to maintain the cultural hierarchal rank within the Tongan community. Only one participant (7%) was not sure about this concept. The one participant (7%) who answered 'Unsure' for this question, (This participant was a church minister), informed that: *Kamata pē ke ma'ama'a ki he kakai e tukufakaholo*. [translation by author] Cultural traditions are not as important to the Tongan people now as it used to be.

The responses of the participants who agreed to maintain the hierarchal rank are summarised as:

- *Ko e 'ilo'anga ia 'o e Tonga ko e faka'apa'apa, lototō, tauhi-vā. Ko e tupunga ia ho no ui ko e* Friendly Island. [translation by author] Tonga

is recognised by respect, humility, and loyalty. That is why Tonga is known as the Friendly Island.

- *Ko e muimui ofi kihe tala ʻo Tonga, pea ko e founga ia te ne tokoni ke fakafepaki ha faʻahinga palopalema*. [translation by author] To closely follow the Tongan culture is the only way to counter any issue.
- *Ko e kakai Tonga ʻoku nau tauhi fonua pea kapau e tuʻutuʻuni e kakai maʻolunga ki he kakai ke nau fakahoko ha ngāue ki he lelei fakalukufua e kakai e fonua pea ʻe talangofua ki ai e kakai*[i]. [translation by author] Tongan people are land-keepers (*tauhi fonua*) and if any message from higher authorities to work for the whole benefit of people than they could agree with this message.

5.6.11 Summary Hierarchal Rank Analysis

With the results discovered, the message delivered from the higher people at the top of the hierarchy triad (e.g., church ministers or nobles) supported by the participants to be a powerful tool for the community. Higher authorities gain the power to deliver messages for the communities to be aware of ICT developments and their consequences. Also, the majority, 93%, (13 participants) supported the idea to maintain the hierarchal rank as an ongoing process of Tongan cultural preservation.

The responses from the participants highlight some of indigenous cultural experiences such as;

- *Kakai tauhi fonua*: *kakai* means people; *tauhi* means to look after or take care of; and *fonua* means land and or people. As always practised in Tongan ways of living, the commoners' *tauhi* (take care of) *fatongia* (duty or obligation) to the king and nobles.
- *Muimui ofi ki he tala ʻo Tonga*: *Muimui* means to follow; *ofi* means close or near; and *tala* means to tell or command. In this situation, commands from the higher authorities (e.g., *nopele* (noble) or *faifekau* (church minister)) are honoured and closely followed by the people. In other words, people are *talangofua* (habitually obedient) to the *tuʻutuʻuni* (command) from higher authorities.
- ʻ*Ulungaanga faka-Tonga*: ʻ*Ulungaanga faka-Tonga* means Tongan culture. A well-known part of the *ʻulungaanga faka-Tonga* is the Golden Pillars

- *faka'apa'apa*, (respect) *lototō*, (humility and generosity) *mamahi'ime'a*, (sense of responsibility) '*ofa*, (love) and *tauhi-vā*, (loyalty and commitment). Tonga is very unique because of these Golden Pillars.

- '*Otumotu Anga'ofa*: '*Otumotu Anga'ofa* means Friendly Islands and it is referred to the warm heart and '*ofa* of the Tongan people.

5.6.12 Tongan Language (Lea Faka-Tonga)

ICT development assists Tongans to connect overseas with families, watch the outside world from home, online banking money transfers to Tonga/overseas without the need to visit the bank. However, on the other side, several damages happen to the formality of the Tongan language. For example, short writing with the incomplete spelling of words (e.g., the word *tangata* (man) which short written tgt, sio (see) – short written using co, *telefoni* (telephone) – short written using pH, etc), the mixture of Tongan-language with English language, non-usage of macron, definite sign, and comma and so on.

A question asked (see Question 58 in *Appendix 12*): *Do you think that the structure of Tongan-language is affected by ICT as defined above?* The answer to this question is summarised in the table below.

Table 24: ICT disrupts Tongan language

Category	**No. of answers**	**Percentage (%)**
Strongly Agree	5	36%
Agree	6	43%
Unsure	0	0%
Disagree	2	14%
Strongly Disagree	1	7%
Total	**14**	**100%**

Table 24 reveals the highest portion, 43%, (6 participants) agreed, and 36% (5 participants) showed that they strongly agreed with the idea that ICT affects Tongan Language. That means 79% (11 participants) agreed/strongly agreed with the effect of ICT on Tongan language. Only 21% (3 participants) disagreed and strongly disagreed with how ICT affects the Tongan language.

Another question asked (see Question 59 in *Appendix 12*): *How about the online posting of swearwords used by Tongans? Do you believe that posting swearwords affect the Tongan values?* (*faka'apa'apa*, (respect) *lototō,* (humility and generosity) and *tauhi-vā*, (loyality and commitment), *mamahi'ime'a* (sense of responsibility) and '*ofa* (love). The answer to this question is summarised in the table below.

Table 25: Online swearwords affect Tongan golden values

Category	**No. of answers**	**Percentage (%)**
Strongly Agree	11	79%
Agree	3	21%
Unsure	0	0%
Disagree	0	0%
Strongly Disagree	0	0%
Total	**14**	**100%**

Table 25 shows that only two choices were made on 'Agree' and 'Strongly Agree'. Therefore, 100% (14 participants) agreed that Tongan golden values of *faka'apa'apa, lototō, tauhi-vā, mamahi'ime'a* and *'ofa* are affected by online exposure of swearwords through social media. There are more comments from the survey participants at the end of this section to show their dissatisfaction about the online posting of swearwords.

A question asked about using the Tongan language posted on social media to affect being loyal to the King and nobles. The hierarchal structure has deteriorated because of ICT. The question asked; *Do you agree with this idea*? (see Question 61 in *Appendix 12*).The answer to this question is shown in the table below.

Table 26: Tongan posters in social media degrade hierarchal rank

Category	**No. of answers**	**Percentage (%)**
Strongly Agree	8	57%
Agree	3	21%
Unsure	0	0%
Disagree	3	22%
Strongly Disagree	0	0%
Total	**14**	**100%**

Table 26 shows that only 22% (3 participants) disagreed with this idea. The highest portion of 57% (8 participants) strongly agreed, and 21% (3 participants) agreed that Tonga people deployed ICT, in terms of social media and online sources to affect the hierarchal structure to nobles and the state of being loyal to the King of Tonga. In summary, 78% (11 participants), stepped ahead to show their dissatisfaction with these online posters on Facebook and social media.

Other participants take further comments to clarify their feelings towards the misleading and untruth texts posted on social media to put down the King of Tonga and his royal family by other unidentified Tongans. These are comments from the participants:

- '*Oku ou fakame'apango'ia he kakai pehē pea 'oku mamahi lahi hoku loto/ he ta'e 'ilo kita mo e fieme'a. Fiema'u ke te 'ilo hoto tu'unga – 'Ilo 'e kita Kita*. [translation by author] I bitterly regret that some people are snobbish and could not be able to realise the right thing they should do. It is significant that we know who we are, and where we stand.
- '*Oku 'ikai ke fu'u ongolelei 'a 'enau me'a 'oku hokoo he taimi lahi, he 'oku 'ikai ke mahino pea 'oku 'ikai ke fakapapau'i 'oku mo'oni*. [translation by author] An uncomfortable sensation of how the scammer performed many times and it is not clear whether is true.
- '*Oku 'ikai keu poupou'i e fa'ahinga 'ulungaanga ko eni*. [translation by author] I am not supporting this sort of behaviour.'
- *Loto mamahi 'aupito. Kuo 'ikai ke 'ilo 'e he kakai 'enau ngata'anga. Kuo nau fai e me'a ngali kovi mo 'ikai faka-Tonga.* [translation by author] Very disappointed. People do not know their limit. They behaved poorly which is very un-Tongan.
- *Ko e me'a fakamamahi lahi 'eni kiate au.* [translation by author] For me, it is very disappointing.

Another open question asked about the appropriate style of writing. Tongan people performed appropriate style of writing which overall affected the Tongan language. The question said; *What sort of feeling for these people for not following the proper ways of writing*? (See Question 63 in *Appendix 12*). Please explain your feelings.

Here are the participants' responses to the question:

- ‘*Oku ‘ikai ke u poupou‘i hono ngāue hala‘i ko eni e lea faka-Tonga*/. [translation by author] I am not supporting the improper use of Tongan language.
- *Loto mamahi lahi ‘aupito*. [translation by author] Very disappointed.
- *Loto mamahi. Ko e maumau pe fa‘unga ‘etau lea faka-Tonga, ko e mole ia ‘a hotau Tonga*. [translation by author] Disappointed. Once the structure of our Tongan language is disrupted, our identity as a Tonga is lost.
- ‘*Oku fakamamahi he ‘oku uesia e hakotupu ‘o e fonua he palopalema*/ *ni. ‘Oku to e fakalahi ngāue kiate kimautolu kau faiako ‘i hono fakatonutonu mo to e feinga ke ako‘i e fanau ‘i ‘apiako ‘i he fa‘unga ‘o e lea faka-Tonga lelei mo totonu*. [translation by author] It is very disappointing, as this issue affects our youth. As teachers, it creates more work to teach the children, the correct structure of Tongan language.

5.6.13 Summary of Tongan Language Analysis

Based on the results collected, there is evidence that Tongan-language is precisely affected by ICT. The majority, 79%, (11 participants) agreed that ICT overall influences the structure of Tongan-language such as short writing of sentences and words, mixing of Tongan-language with English language, non-usage of macron, definite sign, and comma and so on. Also, the overall 100% (14 participants) agreed that posting of swearwords on social media affects Tongan values.

Participants also showed their dissatisfaction of Tongan mask-posters who posted swearwords direct at higher officials and the King of Tonga. Overall, 78% (11 participants), moved forward to challenge these unethical online posters on Facebook and social media.

A teacher stepped forward to express dissatisfaction in misusing the Tongan-language which affected the students and resulted in putting more tasks for teachers. One former high-school teacher said: ‘*Oku ou faka‘amu ke fakamamafi‘i e tohi totonu mo puaki totonu etau lea, ko etau koloa ia. Pea ‘e kamata pe mei ‘api hono ako e fanau ke ‘ilo lelei e anga e tohi mo e lea pea toki hoko atu ai ki apiako mo e komiuniti*. [translation by author] I wish to enforce the appropriate way of writing

and the right pronunciation of words as it is our treasure. Also, to start teaching the children at home to know well on how to read and write and then continue to the school and community.

5.7 Religious Belief

This section aims to discover victims in the church community, and also tries to find out the power of the People of God (PoG). The main idea behind this context relates to the words of the church ministers, church stewards, and church leaders. To measure the words of the PoG, whether it is powerful to assist the process of mitigation OS not only in the church community but also the Tongan community.

5.7.1 Words of *Faifekau*

Section 2.11 discussed the words of *Faifekau* (Church Minister) in the Tongan community. Church and religious belief are some of the major backbones in Tongan ways of living. *Faifekau* and *setuata* (church steward) are believed by Tongans as the representative of God or People of God (PoG). In the Tongan context, the bible messages delivered by the PoG must be prioritised, honoured, and followed as a representation of believing in God. Without following these bible messages is an act of non-Christian and against the Word of God. The advice and message from the PoG to the Tongan people are believed to be a strong message for Tongans to stay righteous and be aware of evil doings. For example, trying to victimise innocent people to fall into difficulties is an act of *angahala* (sin) that leads to *mala'ia* (bad luck). The wages of *angahala* is death.

The first question in this section asked (See Question 45 in *Appendix 12*): *If the PoG delivers messages to the people to be faithful and keep away from cybercrimes, do you think Tongan people will accept the message*? The answer to this question is summarised in the table below:

Table 27: Message from Faifekau

Category	No. of answers	Percentage (%)
Strongly Agree	7	46%
Agree	4	27%
Unsure	3	20%
Disgree	1	7%
Strongly disagree	0	0%
Total	**15**	**100%**

Table 27 shows that the minority, 7%, (1 participant) disagreed with this idea and 27% (4 participants) were unsure of the right answer for this question. The largest portion, 46%, (7 participants) strongly agreed and 27% (4 participants) agreed with this idea. In summary, the majority 73% (11 participants) agreed that the idea that words of the PoG are very powerful.

The *faifekau* and religious officials acquire the power to deliver messages to the people to keep away from cybercrimes.

The second question asked about the action of scammers delivered to Tongans and non-Tongans as a sin, which is opposed to the Christian belief (see Question 47 in *Appendix 12*). The answer to this question is summarised in the table below. The number of participants was reduced to 14 people as one participant refused to answer this question.

Table 28: Online Scamming is a sin

Category	No. of answers	Percentage (%)
Strongly Agree	12	86 %
Agree	2	14%
Unsure	0	0%
Disagree	0	0%
Strongly Disagree	0	0%
Total	**14**	**100%**

Table 28 highlights the majority (86%) (12 participants) strongly agreed, and 2% (2 participants) agreed with this concept. That means that overall, 100% (14

participants) agreed with the idea that the fraudulent acts of scamming the Tongans and non-Tongans are sins and against the Christian beliefs of Tongan people.

The third question asked about the Christian belief of Tongans. The question says; *Do you think that religious beliefs in God will assist Tonga in reducing the problem of online scamming*? (See Question 49 in *Appendix 12*).

The answer to this question is summarised in the table below. The number of participants was reduced to 13 people as two participants refused to answer this question.

Table 29: Christian belief is a defensive tool

Category	**No. of answers**	**Percentage (%)**
Strongly Agree	6	46%
Agree	5	38%
Unsure	1	8%
Disagree	1	8%
Strongly Disagree	0	0%
Total	**13**	**100%**

Table 29 shows that one participant (8%) disagreed with the Christian belief to assist in reducing OS, and one participant (8%) was unsure of the answer to this question. However, the highest portion, 46%, (6 participants) strongly agreed, and 38% (5 participants) agreed with the concept of Christianity. That means the majority, 84% (11 participants), agreed with the idea that Christian belief in God assists Tonga in reducing OS.

This is an interesting response from one participant who disagreed with the concept of Christian belief:

> '*Oku lolotonga fele 'a e talanoa fakalotu fa'ahinga kehekehe 'a e kakai he Facebook. Ka 'oku sio au ki he palopalema 'oku 'alu pe ia ke fakautuutu. Kou sio au ko e palopalema fakasaikolosia…ko e tonounou 'a e 'ilo kita mo hoto Tonga/. 'Oku ne fakafaingofua'i 'e te 'ulungaanga fakataautaha ke te siokita 'ikai sio kihe nofo 'a kāinga mo e Tonga/*. [translation by author] There are many different kinds of religious conversations and advice on Facebook. In my opinion, this is a psychological problem where

some people are selfish, individualistic and lack cultural knowledge to live as Tongans.

5.7.2 Summary of Religious Belief Analysis

The outcome collected in this section supports the fact that 'Tonga is a Christian nation.' According to Niumeitolu (2007), Tonga is known as "*ko e fonua lotu 'eni"* ("this is a Christian nation") (p. 7). Listed below are the answers to support the conclusion that 'Tonga is a Christian nation'.

- About 73% supported the idea that the words of the *faifekau* are very powerful. Any message that comes from the *faifekau* to the people is important and should be followed.
- About 80% believed that online scamming is a sin. The action of cheating Tongans and non-Tongans is '*angahala*' (sin) and the penalty of *angahala* is death.
- About 74% supported the idea of Christian belief or belief in God is a powerful tool to mitigate the issue of online scamming. The process of following the *Tokāteline faka-Kalisitiane* (Christian doctrine) is a strong defensive tool to assist Tonga in reducing OS.

Based on the information mentioned above, the words of the church leaders and strong belief in *Tokāteline faka-Kalisitiane* (Christian doctrine) are tools that can be used to assist in reducing OS in Tonga.

5.8 Cyber-grooming

Cyber-grooming is discussed in Section 3.3.6. The second last part of the survey focused on the online abuse of females. Participants were selected from unmarried single females. Only five (5) females participated in this survey. The purpose of this part is to investigate if there is any online abuse of unmarried single females. It is about online contacts from outsiders to form an online relationship for duplicitous purposes. To investigate the tactics used by outsiders to send friend-requests for fraudulent online loving relationship purposes that may result in potential harm to the target participants.

5.8.1 Responses from participants

A question asked (see Question 8 in *Appendix 11*): *Have you ever been contacted by someone through the internet and requested to be your friend?* About 4 participants accepted the friend request and only one participant answered 'No'. The participant who answered 'No' wrote in the question sheet that 'I do not want to be friend with scammers.'

On the other side, other participants stepped forward to give reasons for accepting and not accepting the incoming request. Details are summarised below:

- 'The requested person is not a close friend or a close relative of mine, so I do not accept the friend request.'
- '… he was my classmate here (Tonga) before they migrated overseas.'

5.8.2 Positive feedbacks from participants

One of the survey participants, a single female, reports the relationship between (her) and her boyfriend. An online growing relationship with an overseas female male for more than three years. It was up to a stage of trusting, assisting, and sharing each other such as mobile top-up, sending items and online transfer of money. The participant quoted about their relationship as mentioned below:

> 'Still going on strong. We help each other out a lot.'

The highlight of this relationship was the long-term plan to be a future husband and wife – marriage.

Another participant experienced a similar story and up to a peak of sharing items and money. The participant quoted:

> 'Since he/she is a person, I know and trust; I will accept and lend money or materials to him/her if needed'

The differences between these two friendships are; the two individuals knew each other before, while the other two friends (discussed above) were not physically met face-to-face with each other, and the relationship is coming to marriage.

5.8.3 Issues encountered by participants

The skills and ICT experiences of the participants were able to identify the lured bait delivered by scammers. There were quick responses from the participants to

deny accepting the friend requests in the initial request halted any further issues that may be encountered in the future.

These issues were related to the lured bait delivered by outsiders. Listed below are comments/quotes from the participants about the unethical approaches delivered by cyberattacks.

> '…. these people are annoying as they video call me showing their naked bodies plus send me naked photos.'

In response to the abovementioned unethical issue, the participant answered in the questionnaire by saying that:

> These people do not frighten me, I just take them as people with mental disorders who forgot to take their pills…… No need to report to the police, not sure how the police here in Tonga will handle this, as these people are from overseas. I just block them.

Another approach performed by a scammer was making good stories. *Figure 44* summarises the makeup story from an outsider. The participant's answer was cut and pasted as summarised below.

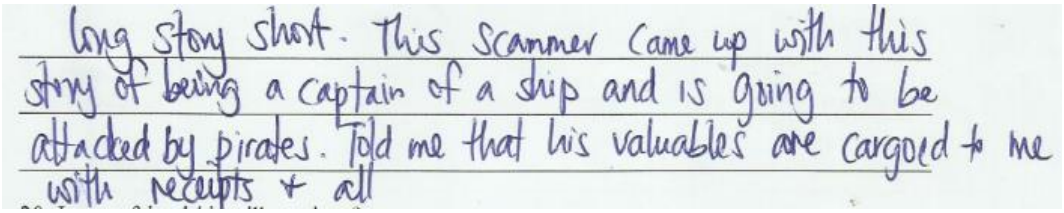

long story short. This scammer came up with this story of being a captain of a ship and is going to be attacked by pirates. Told me that his valuables are cargoed to me with receipts + all

Figure 44: A make-up story from scammer

In response to the above-mentioned good story performed by the outsider, the participant quoted:

> 'I know a scammer and can smell it tricks miles away.'

5.8.4 Summary of Cyber-grooming Section

Multiple types of lure baits such as naked bodies, naked photos, and made-up stories performed by outsiders but the five participants (single and unmarried females) were never failed and victimised. It is discovered from the collected results that the participants were able to identify the incoming requests from outsiders targeted for fraudulent purposes.

Here are some important comments to be noted - ‘I don’t accept friend requests from people I don’t know’; ‘I just block them’; ‘… people with mental disorders who forgot to take their pills’; I know a scammer and can smell it tricks miles away’. These comments testified the ICT skills and experiences of the participants which reflected on the result of zero cyber-grooming or no cyber-abuse case in Tonga.

Another good reflection contributes to building trust between outsiders and participants. These trusts reached a stage of sharing items and money and arranged to meet face-to-face with each other. The highlight of this section was the formation of an intimate relationship. It was up to the climax of reaching the next version of life – a marriage arranged to be coming soon.

5.9 Significance of this research

This is the last and shortest part of the research and it highlights the responses, plans, and change of behaviour of the participants after this interview.

The first question in this section asked (see Question 91 in *Appendix 10*): *Do you think this research is important for Tonga*? The answer to this question is summarised in *Figure 45* as shown in the pie graph below. Participants selected to answer these questions were selected from the GoT and people (n = 119). The majority, 97%, (115 participants) agreed that this research is very important to the nation of Tonga. Only 3% (4 participants) provided no answer to this question.

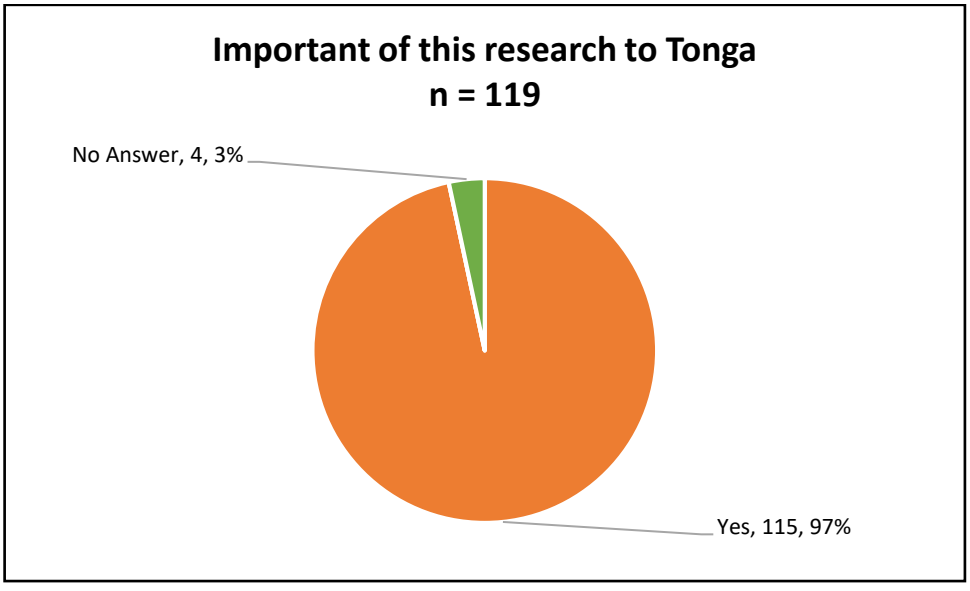


Figure 45: Important of this research

Another question asked the participants about plans to overcome the existing, and future issues related to OS. In response to this question, the participants from the GoT and people (n = 119) responded and provided plans as shown in the table below.

Table 30 reveals that 66% (78 participants) implemented plans and 20% (24 participants) did not have plans to mitigate OS. About 14% (17 participants) did not attempt to provide an answer to this question.

Table 30: Plans to overcome OS

	People	**GoT**	**Total**	**Percentage (%)**
Plan	54	24	78	66%
No Plan	17	7	24	20%
No Answer	17	0	17	14%
Total	**88**	**31**	**119**	**100%**

Here are some of the plans provided by the survey participants to assist in fighting against online scamming:

- The best plan I think is more education for parents and children and everyone including church leaders. It is not only youth or children because even adults too can fall into this trap. Also for those experienced in using the internet to stop putting up all the personal details on the internet. In my organization where IT security is very high, we are only allowed to use WEBEX in our system and not others like ZOOM, as it is not safe for your details. Well, that is what we are advised to do.
- Implement cyber safety as part of the school curriculum to be taught in school and educate young people as they are the future generations of Tonga and need to be aware of it.
- To employ an ICT person in the organisation that have the skills and knowledge on these issues to inform and look after the ICT system of the organisation
- The main issue is a lack of understanding and awareness of the vulnerability of private and confidential information when the system

is not protected from the outside world while you are connected online to the internet. The plan is to set up a strategic action plan with activities and timelines of implementation to address the above issue and the related ones as well.

- I think the more workshops and training for all people of Tonga just to get an understanding about online scamming or scams the better, I will benefit from reducing problems not only for older people who are not familiar with the internet but for younger generations who still learn about using the internet. More qualified ICT workers and staff to conduct any training or work for people, better firewall with update and strong Antivirus etc. and also with protected environment.
- Phishing has been an on-going issue. The Ministry has been dealing with since a few years back. We have put in place internal policies for checking suspicious emails however, there still needs to be on-going training for the staff regarding this issue to prevent this from occurring again.

5.9.1 Summary of plans

Survey participants suggested several points as plans to tackle existing and future issues about OS. A table is created to summarise all the plans suggested by the participants.

Table 31: Summary of participants' plans to mitigate OS

	Total	**Percentage (%)**
Education/ workshop/training	31	30%
Enforce IT personnel/ law/policy	20	20%
Self-awareness	16	16%
Update software	9	9%
Seek/hire IT expert	8	8%
Strategic plan	8	8%
Share of ICT knowledge	4	4%
Include cybersecurity in school syllabus	3	3%
Treaty with other wealthy nations	2	1%
GoT to provide sufficient budget	2	1%
Total	**103**	**100%**

As the question was open to answer as many as possible, participants contributed more than one answer to show their plans. The total number of plans (n = 103) together with the summary of plans are provided in *Table 31*.

- *Education/ workshop/training*: The highest portion, 30%, (31 votes) suggested by the participants to send students overseas for cybersecurity training, and to provide workshops and training within government organisations and communities.
- *Enforce IT personnel/law/policy*: This plan is not only focused on law enforcement and policy but is also for the Tongan people to be well equipped with ICT knowledge and follow the law. About 20% (20 votes) suggested enforcing IT personnel, law, and policy.
- *Self-awareness*: About 16% (16 votes) believed that self-awareness is a good plan. Self-awareness involves self-understanding and knowledge of proper link and attachment to open, identifying email scams, the integrity of online payments, and other online acts.
- *Update software*: About 16% (16 votes) suggested upgrading of software as one of the plans to monitor. Upgrading of software involves adding new security and removing outdated features to computer devices.
- *Seek/hire IT expert*: Participants preferred to seek assistance and hire cybersecurity experts to monitor the IT systems. About 8% (8 participants) agreed with this plan.
- *Strategic plan*: To implement long-term plans with the vision to achieve the goal of maintaining a cyber-safe environment. About 8% (8 participants) voted for the GoT to implement a long-term vision for cyber-safety in Tonga.
- *Share of ICT knowledge*: As cybersecurity is a new era for Tongans, participants requested local people who gained some ICT knowledge to share the experiences with other illiterates. About 4% (4 participants) voted and requested assistance to share ICT experiences of locals within Tongan communities with other non-cybersecurity literate.
- *School syllabus*: About 3% (3 votes) requested to include cybersecurity in the school curriculum.

- *Treaty*: As Tonga is still a developing nation, two (2) participants initiated the idea of binding formal agreements with other ICT developed nations. The treaty will open gateways to assist in developing cybersecurity matters in Tonga.
- *Budget*: Two (2) participants also raised the importance of supplying enough funds for the government organisations to manage cybersecurity.

The final question asked (see Question 93 in *Appendix 10*): *Now that we have finished this interview and you have answered these questions, do you think you are more aware of possible scams? How do you think your behaviour will change because of this interview?*

Here are the responses from the participants:

- I receive a lot of scam emails, but I choose not to read because I have my ways of being very selective of what emails I want to read first and to the response. And so I am not concerned about the spam because I see it every day and I delete it immediately. But honestly, I realise now that people who may be vulnerable based on the situation they are in: perhaps new to the internet, or desperate for $$ will end up being serious victims of Scams.Other populations are children and young girls who do not experience life and will fall into trap of sexual abuse. This can cause death but can be prevented as long as people like parents, teachers, church leaders, village leaders, youth leaders, government leaders are aware and are outspoken or outreach to their audiences.
- Your research has also brought awareness to me on how my friend was scammed when we studied in PNG twenty years ago. She received a phone call telling her that it was my cousin's family. My cousin's mum was from PNG and that boy lied to my friend about his name. He called her and talked for hours and hours on the public phone. He sent a photo of him to my friend, and it was an old photo of an Indian-like youth. My friend falls for the picture. It was okay in the beginning but because this was a college and we only had one public phone where you put the coin and call your parents, we started feeling frustrated about that imaginary guy. I told my friend off but because the guy had a sweet

voice and a false photo of a nice Indian youth, my dumb friend hated me more and gossip about me to that guy. That guy even swore at me to her, and she comes and tells me as if I care because I never see that fake friend. She was emotionally affected and was always in the room because of this scam. She did not believe me and started hating me. We were only two girls from home, but she would trust that fake friend more than me. Luckily, we have sponsored a student with a low allowance, so she never sends $$ to him. And lucky our school was very strict to allow overseas students out, so she did not have to be that crazy to fly over to her fake friend just to be murdered or who knows. Also, we had to live on the campus straight to the airport to be dropped by our college driver, so this guy never met my friend physically.'

- 'I am thankful for this research and I hope that you will interview some right people who were victims to answer some questions that did not apply to me.
- As from all the question that states the importance of keeping myself from scams etc, we all very aware of our people especially those that have no idea of scams and using the internet, we should survey for all Tongan people, seminar, training just to give them a hind of keeping themselves from being cyberbully and cyberattack also scams with fraud. I encourage all ICT to share their knowledge for a better digital environment for Tonga, the more we learn the better our surroundings.
- I would be more careful with checking email and responses to unidentified senders. I would also help those that I love to do the same thing for their safety.
- *Koe ako lahi 'eni koe'uhi koe issue ko eni pea 'oku to e fu'u kakaha ange he taimi ni pea 'oku mahu'inga ange ke consider he pule'anga pea moe ngaahi potungāue 'a e cyber security ke tokoni ki hono malu'i ` ae kakai meiha mole ha pa'anga, pea koha ngaahi palopalema kehekehe 'e malava ke fakatupu mei he ngāue 'a e kakai kākā ko eni 'oku fai.* [translation by author] This is a big study for me because this issue, is even more intense, now and it's more important for the government to consider cybersecurity services to help protect people

from losing money, and avoid a variety of potential problems that could be caused by these fraudulent people.

- *Ka ʻoku ʻi ai ee fakaʻamu ʻe tokoni lahi ho ako ki he ngāue ʻoku mau fai he ko e palopalema ʻena kuo hoko pea ʻoku ʻalu pe ke lahi ka ʻe hoko ho fekumi ʻoku fai ke tokoni mai ki he ʻetau kiʻi fonua masiva.* [translation by author] There is hope that your education will assist our work as this problem has occurred and it is increasing. But your research will help us out in our poor country.
- With the entire question being asked, I am more aware that scams are real even though I am not yet a victim. I believe it is important to first understand what scamming is, what it does, and the consequences that it may affect us. Regarding my behaviour I think I will be more aware and careful of using the internet at home and also at work as well. Not only that but giving of my personal information on the internet and being more careful in opening a link that is sent to my email. It is also crucial to raise awareness here in Tonga for people to understand and know scamming does exist.

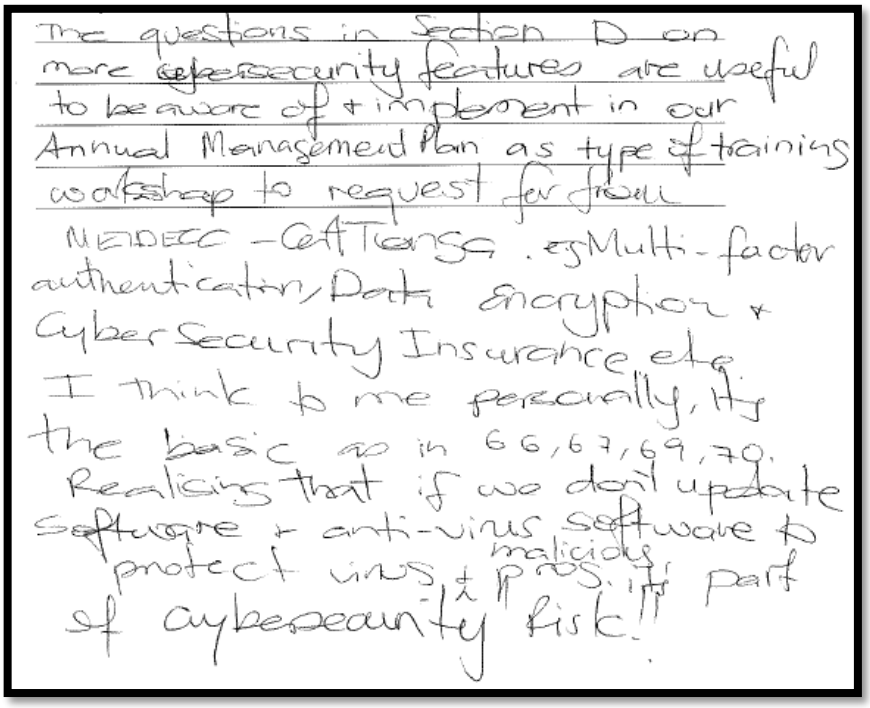


Figure 46: Response about the significance of this research

Figure 46 is a response from one of the civil servants. The participant informed that Section D (Cybersecurity features) on the questionnaire are useful elements. These cybersecurity features will be implemented in their organisation Annual Management Plan.

The above-mentioned answer is re-written to be clear: 'The questions in Section D on more cybersecurity features are useful to be aware of and implemented in our Annual Management Plan as a type of training workshop to request for from MEIDECC (Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Climate Change, and Communication) – Cert Tonga . E.g., Multi-factor authentication, Data Encryption, Cybersecurity Insurance, etc. I think to me personally, it is the basic as in questions 66, 67, 69, and 70. Realising if we do not update software and anti-virus software to protect against virus and malicious programs, it is part of the cybersecurity risk.'

5.9.2 Analysis Summary

Data Analysis is the largest (80 pages) and crucial section of this project. Some major issues (travel bans and data collection) were encountered during this process but in the end, it was finally enabled to collect data from 139 participants from Tonga. The number of participants was expected to be higher than 139 participants. However, the data collected from this number of participants were able to analyse and provide relevant information for this project.

There are three main highlights to be acknowledged in this section. 1) The deployment of *e-fanongononga tokoto* (e-ft) methodology to challenge the existing issue of travel restrictions due to COVID-19. The provision of e-ft methodology was able to communicate and collect information from the survey participants. 2) The availability and willingness of these 139 participants to partake in this survey are honoured and acknowledged. Without these participants, this project is not yet coming to this stage. *The ability to answer the three core questions of this thesis is achieved.* The information collected from the survey participants proves that online scamming was and is currently happened in Tonga and there are possible solutions to solve this issue.

CHAPTER SIX

6. DISCUSSION

6.1 Introduction

The first part of this section highlights the methodology designed to interact and collect data from the survey participants. A strategic electronic communication technique to challenge the main worldwide issue of COVID-19 and travel restrictions. A deployment method to interact with the survey participants from Hamilton, New Zealand, to connect with Tongan people in the South Pacific.

The second part focuses on key findings discovered in this research and ensures the survey findings are interrelated and answers the three main questions that were planned to guide this thesis. Here are the three main questions:

- How has rapid ICT deployment in Tonga influenced online vulnerabilities?
- How is the incidence of malicious cyber-events in Tonga exacerbated by aspects of Tongan culture?
- What strategies have been identified by the research to improve ICT security in Tonga?

6.2 e-fanongonongo tokoto (e-ft)

The electronic method is e-ft, a relatively inexpensive option, allowed access to otherwise unreachable overseas participants. An e-ft methodology was originally developed as a second option, however, with the rise of COVID-19 came to be considered the best and most cost effective solution. The method involved connecting with survey participants through Facebook, Facebook Messenger (FM), Email and Zoom. In addition to saving time and money in overseas travel and associated quarantine restrictions, it reduced the exposure to a range of environments that may have negatively affected health.

One of the advantages of e-ft is the extension of the research area to reach the whole five regions of Tonga. As discussed previously, the initial plan was to physically visit the three main regions only (Tongatapu, Vava‘u, and Ha‘apai), excluding the two other islands (Ongo Niua and ‘Eua). The deployment of e-ft methodology outreaches to all provinces of the entire Kingdom of Tonga. The inclusion of all

provinces enforces the integrity of data collection and research findings by collecting data from their ends. All the voices, thoughts, and issues about the cybersecurity of all five nations in the entire Kingdom are received and recorded in this research.

The primary focus of the application of e-ft relates to discovering an online scam in the furthest region in Tonga. Without e-ft, there would have been no opportunity to discover and record the cyberattack that took place at the Ongo Niua, the last and furthest islands in the North of Tongatapu, the main island capital of Tonga. The achievement of the e-ft was based on the collaboration of the researcher with the survey participants and Good Samaritans (GSs). As discussed previously, GSs refers to six Tongan citizens who assisted in delivering questionnaires to the participants and returned them to the researcher without costs involved. Also, former New Zealand tertiary students (including UoW alumni) contributed a lot to e-ft by delivering and propagating the survey questionnaires to other participants. The e-ft looks promising for a future method for collecting data without physical visits overseas but to communicate with the outside world from the home or classroom.

6.3 Summary of research key findings

The subsections below summarise some of the key findings discovered in this research. The information collected from the survey participants has the potential to answer the three fundamental questions of this thesis. The first essential question to guide this thesis says*: How has rapid ICT deployment in Tonga influenced online vulnerabilities?* Before answering this fundamental question, the first step is to clarify the existence or non-existence of online scamming (OS) in Tonga. If OS has occurred in Tonga, then we needed to investigate the reasons that cause the Tongans to fail to OS or cyberattack, including the tactics that are deployed by scammers to cause vulnerability.

6.3.1 Is online scamming occurring in Tonga?

Yes, Tonga was and is currently impacted by OS. It is clear from the research findings that OS started before 1990 on the two main islands of Tongatapu (the capital) and Niuatoputapu, while the regions of Vava'u, Ha'apai, and 'Eua have remained unaffected. Cyberattacks have occurred every day and at all times of the

day and night, with multiple attacks frequent. Moreover, between 1990 and 2020, fourteen Tongan residents lost anywhere between TOP $100 to the range of TOP $5,001 – TOP $10,000. The ages of victims impacted by OS attacks ranged from 31 – 40 years of age.

6.3.2 5 tactics deployed by scammers.

With the majority of Tongans able to access cyberspace using a range of devices, including phones, laptops, desktops, and tablets, scammers deployed five techniques using lured bait to attract the attention of Tongan Innocents (TIs). These were:

- send email from unknown senders
- send email contacts sent via victims' friends
- send links from friends to click and open
- send texts through mobile devices
- make phone calls from unknown individuals.

The first two tactics mentioned above are classified as phishing attacks. *Phishing attacks* were the major attacking tactics discovered in this research. The result collected in Subsection 5.2.6 reveals that the majority (53%) of the tactic deployed by OS to connect with TIs was *email phishing.* The phishing attack is discussed in the Literature Review Subsection 3.3.3. Saberi, Vahidi, and Bidgoli (2007) refer to phishing attacks as "identity theft" (p. 311). Shadden (2005) describes identity theft as acquiring "enough data about another person" for fake purposes (p. 171). The results of the survey in this research on identity theft is discussed in further detail in the next section.

There were four main methods deployed by scammers to gain secret information from TIs. The two major information required was *bank credentials* and *personal detail*. The other two requirements performed by scammers are indirect types of contact. Scammers asked the TIs to answer *survey questions* that were attached to bogus emails. The final request asked to give names of friends and families for further contact. Details of the requested information are listed below:

- *Bank credentials:* account number, username, credit card, etc.

- *Personal details:* name, address, date of birth, IRD number, security number, etc.
- *Survey:* asked to click on a website link, open attachment and answer questions in a survey.
- *People*: asked for names of family members, friends, relatives, and other people.

6.3.3 5 core vulnerabilities.

This subsection is subjected to report the final summary of the core vulnerabilities. In this context, the major failures to OS in Tonga are summed up and named by the researcher as the *5core-vulnerabilities,* which are listed below.

- Greed
- Romantic/love/empathy
- Lack of cybersecurity training
- Lack of ICT knowledge
- Unwillingness to report to authorities

6.3.4 8 lured baits

According to the Thematic Analysis in Section 5.2.15, about 48% (21 out of 44 attacks) were classified as victims that failed to seductive baits enticed by cybercriminals. The collected answers from the survey participants were classified into different classes to define the real meaning of lured baits (see *Table 19).* Based on the type of fraudulent acts and the classification of the collected answers, there were eight (8) types of lured baits delivered by cybercriminals to victimise TIs. In this context, *lured baits* are therefore referred to:

- false promises of exceedingly profitable returns of money.
- fake online cheap items
- bogus emails for fraudulent purposes
- set up of untruthful romantic relationships
- false announcement of lottery winners
- deceitful friend requests
- fake overseas job opportunities
- display of naked bodies/photos

6.3.5 Financial Impacts

As mentioned in Section 6.3.4 (above), lured baits refer to *cheap items, false promises, display of naked bodies/photos, money, romance, lottery winners, friend requests, and overseas job opportunities.* Cybercriminals were targeted to gain personal information using different tactics. The outcome revealed that 9% (7 participants) lost their secret information to scammers. Secret information were bank account number, username, password, credit card, name, address, date of birth, IRD number, security number, and other private credentials). Victims were involved in one, two, three, and more than three times and the worst result ended up in losing money. About 12% (14 participants) were victimised and lost money to scammers ranging from under TOP $100 up to under TOP $10,000 (mentioned previously).

6.3.6 General overview and discussions

As mentioned previously, the first essential question of this thesis says: *How has rapid ICT deployment in Tonga influenced online vulnerabilities?* As discussed on Section 5.1.4, the top three devices deployed by participants to access cyberspace were mobile phones, 33%, (119 participants)), laptops, 24%, (102 participants), and desktops, 24%, (88 participants). Deployment of mobile phones and laptops signifies the transitional transformation of ICT from immobile to portable devices.

With the freedom of the TIs to access cyberspace through computer devices, the top three - mobile phones, laptops, and desktops, the scammers take advantage to exploit TIs. The *5-tactics deployed by scammers* to entice *8-lured baits* to phish for *bank credentials* (account number, username, credit card, etc.) and *personal details* (name, address, date of birth, IRD number, security number and so on) from TIs. Because of *5-core-vulnerabilities,* TIs fell to cyberattack and resulted in the loss of credentials and money.

The online scamming process conducted by cybercriminals to deceive Tonga innocents is 24/7 non-stop attacks, unrestricted to all ages, free to attacks on all regions of Tonga, attacks from lowest to higher people, and no limitation to other Tongan citizens as they (cybercriminal) attack all levels. The entire Kingdom of Tonga is the main target of cybercriminals. *Figure 47* clarifies the actual scamming process that occurred and currently occurs in Tonga.

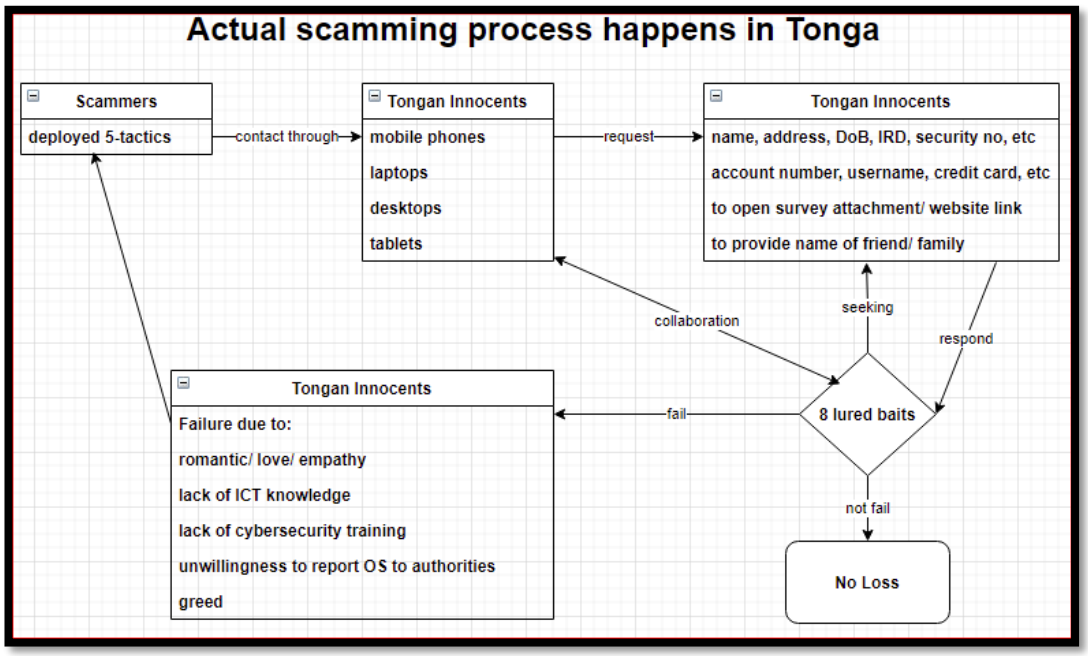


Figure 47: Scammers' pathway to exploit TIs

Figure 47 summarises the pathway and the exploitation process performed by scammers. In the first attempt, the scammers *deployed 5-tactics* by using the top four computer devices to contact TIs. Scammers deployed *8-lured baits* to phish for *bank credentials* and *personal details*. For Tongans who failed to *8-lured baits*, the results led to the loss of credentials and money, and for those who are not fail to lured baits end up in 'No Loss'.

> *The results obtained from this survey are the major backbone and achievement of this research. It discovered that the OS already happened in Tonga due to vulnerabilities. The vulnerabilities are not only technical issues but also human behaviour issues.*

6.3.7 Stumbling block to fight against OS

In addition to *8-lured baits* and *6-core-vulnerabilities* as part of the primary factors of becoming victims to cybercriminals, there are stumbling blocks that contribute to the process of fighting against OS. There is an important case to discuss in this section, which is another contributing factor for fighting against OS.

Unwillingness to report to authorities in Section 5.2.15, encountered by one victim who lost TOP $100 – TOP $1,000 around 1990 – 1999, is another contributing factor to the fight against OS. The victim refused to report to the Ministry of Police

(MoP) or related authorities. The answer from the victim said: '*Thought to just leave as it was as there were some other people involved.*' A clear answer from the victim there were other people (victim's friends) involved in this OS case. The failure to report to the police halts the opportunity to record this case as a cybercriminal case and avoid further investigation.

In addition, the refusal to report can relate to our cultural belief of *'ofa* (love) or *tauhivā* (nurturing relationship). The victim shows *'ofa* and does not agree to go another step ahead (maybe involved with legal action) and still tries to maintain a good relationship with friends. A gain to the victim's friends as no further investigation may involve but, the process of fighting against OS is affected.

6.3.8 Impacts of Tonga culture on OS

The second question of the thesis asked: *How is the incidence of malicious cyber-events in Tonga exacerbated by aspects of Tongan culture?* Again, the focus of this unit concentrates on the influences of rapid ICT on Tongan culture and Tongan concepts. These concepts of the Tongan culture refers to *faka'apa'apa* (respect), *lototō* (humility), *tauhi-vā* (nurturing relationship), *'ofa* (love), and *mamahi'ime'a* (loyalty or sense of responsibility). Tongan concepts refer to *Tahi Kulokula* (Sea of Red), *Mate ma'a Tonga* (Die for Tonga), *Mate pē Tonga he ngāue 'a e Tongan* (Tongans kill Tonga), *fakatu'utu'unga e nofo* (hierarchal rank), *Lea Faka-Tonga* (Tongan-language), and *lotu* (religion).

6.3.8.1 Influences of ICT on Tongan Core Values

These subsections highlight some of the survey findings in Cultural Analysis Section 5.6, which are relevant to answer the second question of this thesis (mentioned above). As mentioned previously, the theme of this section has changed to include both victim and perpetrator. That means for the victims attacked by cyberattacks and Tongan perpetrators who arranged to attack other TIs within the community.

In Section 5.6.1, it summarises two contradicted answers from one participant. A question asked about a perpetrator within the Tongan who performed fraudulent acts to victimise other Tongans. If the perpetrator is well known, relative, or friend of the participant, what is the proper action to do? The question asked: *Are you*

going to report the scammer within the Tongan community to the police/ supervisor/ town officer etc. or you keep it secret and remain silent?

The answer from the participant clarifies that there is no need to report to authorities but to first approach and discuss the case and give advice to the scammer.

> '*Koe'uhi kohoku kainga pē maheni, te u feinga leva ke u 'uluaki talanoa kiate ia fakafo'ituitui pē pea 'oanga ha akonaki kiate ia ki he me'a 'oku ne fai 'oku 'ikai sai.*[translation by author] Because the scammer is my family and friend, I will attempt to take personal discussion and give precautionary advise, and informed him that what he is doing is not good.

Another question asked; how about if the scammer is not a relative or friend of the participant? The same participant responded with a different answer by informing that the scammer must report to related authorities. The participant said:

> 'Because I am not a friend of the scammer and am reluctant to interfere I have to take him to the right place to help this person.'

The verbal discussion between the researcher and the participant to clarify contradicted answers which is unethical and against the religious belief of Tongans. The participant further clarifies that it is more important to *tauhi-e-vā* (action of nurturing good relationship) and to show *'ofa* (love) to the perpetrator by giving another chance. '*Ofa* and *tauhi-e-vā* are parts of the Golden Pillars of the Tongan Culture.

There is a Tongan word called *'ofa-vale*. *Vale* means "foolish, silly, or ignorant" (Churchward, 1959) (p. 533). '*Ofa* is love. '*Ofa-vale* is therefore referred to as 'foolish-love'. In the Tongan context, the failure to report to authorities about unethical or illegal acts is referred to *'ofa-vale*. This may also refer to the unwillingness of the survey participant to report to relate authorities (as discussed above) is due to *'ofa-vale* or foolish-love.

Another answer from a participant in Section 5.6.2 in response to a question in the survey question asked: *What about if this person (scammer) is the leader of the village, noble, church leader, Government leader, or leading officials? What are you going to do*? *Do you still insist on reporting them to the authority and police*?

The participant reluctantly disagreed to report to MoP and higher authority. Here are the three answers quoted from the participants.

> *1). ʻOku ou fakaʻapaʻapaʻi ʻa e tokotaha ni he ko e maʻolunga. 2). ʻOku ou tailiili naʻa hoko ha meʻa ki a kita mo hoto famili. 3). ʼOku puli ʻa e ʻamui, naʼa ko ha tokotaha ʻeni ʻe tokoni ki a kita he kahaʻu.* [translation by author] 1). I respect this person (scammer) due to his high position. 2). I am scared that something will happen to my family and I. 3). The future is unknown, may be this person (scammer) will help me in the future.

According to the answer provided by the participant, the first decision was based on *fakaʻapaʻapa* (respect) to the perpetrators due to their high position in the society (*hierarchal rank*). In respect to the high rank (e.g., *noble, church leader, Government leader, or leading officials*), the participant did not report to MoP and higher authority about fraudulent acts. Although there are other related factors related to the participant's answers such as *fear for the family*, *environmental instability*, and *a wheel of fortune*, the main reason was due to *fakaʻapaʻapa* (respect). *Fakaʻapaʻapa* is one of the key elements of the Golden Pillars of the Tongan Culture.

Due to clear implication of the denial to report to related authorities about fraudulent acts within Tongan communities, the author of this thesis concludes that:

> ʻ*Oku mahuʻinga ange ki he kakai Tonga ke tauhi ʻa e molumalu ʻo e ʻulungaanga faka-Tonga ʻi haʻane lipooti ki he kau maʻu mafai ha ngaahi ngāue ʻikai moʻoni hono ngaueʻaki e ʻinitaneti ke takihalaʻi e kakai e fonua.* [translation by author] It is more important for the Tongan people to be loyal to the Tongan culture than reporting to the authorities about the unethical use of the internet to mislead the nation's citizens.

> *ʻE hoko leva hono ʻikai lipooti ʻa e ngaahi ngāue hala ki he kau maʻu mafai, ko hono holoki e ivi fiengāue ki hono tauiʻi e faihala ʻo e ngāue fakaehaua ʻo e ʻinitaneti/. Pea ʻe ola ia he hokohoko tupu ai pē ki ʻolunga e ngāue halaʻaki ʻo e ngaluope he kahaʻu/. ʻOku fiemaʼu ke ngāue fakataha mo faitotonu ʻa e kakai Tonga ke fakasiʻisiʻi e ngaahi palopalema ni.* [translation by author] Due to the non-report of fraudulent acts to related

authorities, the determination to fight against the internet's illegitimate acts diminish. This will result encourage the growth of internet fraudulent acts in the future. There is a need for Tongan people to work together honestly to fight against this issue.

6.3.8.2 Impacts of ICT on Christianity

There is a change in the theme in this subsection. The change highlights the power of the church through the People of God (PoG), i.e., *faifekau* (church minister), *setuata* (church steward), or *takilotu* (church leader). The ideology prefers to look at the church and the PoG to be crucial factors to either assist in reducing or speed up the spread of OS not only in the church but also in the Tongan community.

According to the results collected, (See Section 5.7) there are great influences of the church in modern Tongan society and rapid ICT development. The positive outcomes support the fact that "*ko e fonua lotu 'eni"* ("this is a Christian nation") Niumeitolu (2007) (p. 7). The philosophy of "*ko e fonua lotu 'eni"* is an appropriate defensive approach to fight against OS.

The survey results (summarised in Section 5.7.2) confirmed the following evidences:

- The majority, (73%), of the participants agreed with the idea that words of the People of God or *faifekau* are very powerful to their church members. They acquire the power to deliver messages to church members or followers to keep away from cybercrimes.
- Cheating other people such as victimising TIs is *angahala* (sin) and the wages of *angahala* is death.
- The *tokāteline faka-Kalisitiane* or *faka-lotu* (Christian doctrine or religious doctrine) is a strong defensive tool for the people of Tonga to fight against the OS.

The influence of *lotu* (Christianity) plays an important role within Tonga. The combination of the strong belief in God and the words of the *faifekau* are very powerful in the Tongan community. Any message from the *faifekau* is an obligation for church members to follow. Christianity and words of PoG are powerful defensive tools to assist in fighting against online scamming in Tonga. Based on

the results collected and the philosophy of *lotu* in Tonga, quotes from participants were gathered together to form one quote that:

> *Ko e lotu ko e mata'i-koloa 'a e Tonga. Ko e ivi mafai 'o e lotu 'i Tonga ko ha me'angaue lelei ke ta'ota'ofi'aki 'a e ngauehala'aki 'o e tekinolosia.. Ko e ngauehala'aki 'o e tekinolosia ki ho no kakai'i e kakai ko e angahala. Ko e totongi 'o e angahala ko e mate.* [translation by author] Christianity is a foremost asset of Tongans. The power of Christianity is an appropriate tool to decrease the abuse of ICT in Tonga. The abuse of technology to cheat people is *angahala* (sin). The wage of *angahala* is death.

6.3.8.3 Impact of ICT on Tongan language

Majority of the Tongan participants (79%) agreed that the structure of Tongan language is affected by ICT. They agreed that there are great influences of rapid ICT development on Tongan Language. In Section 1.2, it discusses Tongan Language and in Section 5.6.12 it summarises the research findings together with the comments and views from the Tongan people. The structural effects involve the short and incomplete writing of words; the mixture of Tongan language with the English language; and the non-usage of macron, definite sign, and comma, etc. For example, the word *tangata* (man) which short written tgt, *sio* (see) – short written using co, *telefoni* (telephone) – short written using pH, etc)

Online posting of swearwords on social media by masked authors both local and overseas affected Tongan Golden values. Section 2.10.1 discusses the *tabu* or *taboo* (forbidden) between *tuonga'ane* (brother) and *tuofefine* (sister) in Tongan culture. Although there is no established law for the *faka'apa'apa 'a e tuonga'ane ki he tuofefine* (respect of brother to sister) but it is a cultural inheritance that exists for ages. Some of the cultural taboo includes no swear or hateful words between sister and brother; and respect or "*faka'apa'apa 'a e tuonga'ane ki he tuofefine … 'Ikai tena mohe ha fale 'e taha*" (Vaioleti, 2006) (p. 28) [translation by author] brother pays tribute to sister … It is forbidden for *tuonga'ane* and *tuofefine* to sleep in one house.

At any stage where no taboo or *faka'apa'apa* between *tuonga'ane* and *tuofefine,* would be frown upon as *'ikai akonaki'i 'e he tamai mo e fa'ee* (not giving the right advice by parents). *'Ikai akonaki'i* is claimed to be the parents' failure to give the

right guidance/advice to the children. *ʻIkai akonakiʻi* leads to *fakamā* (feel embarrassed, uncomfortable, or ashamed) and result in a long-standing rumour for the family. *ʻIkai akonakiʻi* may lead to *ʻikai-fakaʻapaʻapa* (no-respect) between *tuongaʻane* and t*uofefine*.

This is happening today about posting swear words on social media. The freedom of masked internet users to post unethical posts overall affects the *nofo ʻa kainga*. Within the immediate family living, the freedom of *tuongaʻane* and *tuofefine* to access ICT is unlimited. With this freedom and unlimited access to expose and read these unethical posts and the *fakaʻapaʻapa ʻa e tuongaʻane ki he tuofefine* is *ʻikai fakaʻapaʻapaʻi* (un-respected). As this issue is valuable to the *nofo ʻa kainga* and the whole Tongan society, the view of locals and overseas on this matter needs to be addressed. Section 5.6.12 summarises that:

> *Both local and overseas survey participants believed (100 %) that posting swearwords on social media affects the Tongan golden values (faka'apa'apa, lototō, tauhi-vā, mamahi'ime'a, and 'ofa.*

There are questions to tackle this issue as the posters are not identified as they are not using their real names (masked) and located overseas. Is there any way that these masked scammers can be identified? Is there any international cybersecurity law to cope with this issue? Cybersecurity law in the South Pacific Islands is discussed in Section 3.6.3. Part of the discussion in this section mentioned: *The infiltration of cybercrimes is due to inadequate ICT, resistance to cooperating with international law, and the absence of legislation.*

Section 1.2 discusses the impacts of ICT in Tonga. One of the main examples of the discussion was about a disparaging fake text posted on Facebook. The discourteous fake text was directed to the King of Tonga's family. This post no longer exists on Facebook as the GoT promptly banned access to this site. A wake-up call for the Tongan people, and it was up to a time that the GoT decided to ban Tonga from Facebook. Tongan Attorney General and other Tongan officials met with Facebook authorities in Australia in 2019 to discuss this issue and investigate the unknown author. It is believed that the author was a Tongan living in Australia (RNZ, 2019b).

The lessons learned from this unethical behaviour of posting the discourteous fake posts are the non-existence of *faka'apa'apa* (respect), failure of *tauhi-vā* (loyalty and commitment), and breakdown of *'ofa* (love) to the King of Tonga. Additionally, the hierarchical status of the King to remain at the top of the hierarchy triad as the supreme power of the entire Kingdom is *'ikai to e mahu'inga* (no longer valuable). The other point relates to the discourteous fake post about the type of language being informal. Tongan language is divided into three main categories – language for the King, language for the nobles, and language for the *tu'a* (commoners).

A question was asked to the survey participants related to discourteous fake posts and the impacts on the context of the hierarchy triad. About 78% showed dissatisfaction with these discourteous fake posts posted on Facebook and social media. Participants also stepped forward to expose/quote their disappointments about this issue. Some of the quotes from the frustrated participants are shown in Section 5.6.12. However, some of these quotes are also discussed in this section to highlight the disappointment of the survey participants. Here are parts of the quotes:

- I bitterly regret that some people are snobbish and could not be able to realize the right thing they should do. It is significant that we know who we are, and where we stand.
- An uncomfortable sensation of how the scammer performed many times and it is not clear and no clarification of true evidence.
- I am not supporting this sort of behaviour.
- Very disappointed. People do not know their limit. They performed inappropriate conducts and non-Tongan performances.

Again, other participants expressed their feelings on the misuse and inappropriate ways of writing. Here are some of the quotes from the survey participants to show their frustrated feelings:

- It is very disappointing as this issue affects our youth. As teachers, we have more workloads to teach the children to correct and keep the structure of Tongan language accurate and perfect.
- Disappointed. Once the *fa'unga* (structure) of our Tongan language is smashed, our identity as a Tonga is lost.
- I am not supporting the improper use of Tongan language.

6.3.9 Strategies to mitigate OS

The third and final question of this thesis asks: *What strategies have been identified by the research to improve ICT security in Tonga?* Section 5.9.1 highlights the summary of plans written and suggested by the survey participants on their answer sheets, to be implemented in Tonga. The survey participants suggested in their plans to:

- provide education/ workshop/training
- enforce IT personnel/ law/policy
- self-awareness to differentiate right and wrong
- update software
- seek/hire IT expert
- provide cybersecurity strategic plan
- local cybersecurity experts to share their ICT knowledge with other Tongans
- include cybersecurity in the school syllabus
- form treaty with other wealthy nations
- provide sufficient budget

Section 1.4 highlights eleven (11) recommendations submitted to the GoT by Laulaupea'alu and Keegan (2019). Some of these recommendations are noted to be akin to the strategic plans provided by the survey participants. These eleven recommendations are reposted in this paragraph to compare the similarities with the new suggestions/plans provided by Tongan survey participants. Here are the recommendations that the authors (Laulaupea'alu and Keegan) proposed to the GoT to deploy the following cybersecurity features:

- Penetration Testing (PT)
- Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP)
- Budget
- Cyber Insurance
- Cyber Security Experts
- Information Security Policy (ISP) & ISO
- Data Encryption
- Data Backup
- Two Factor Authentication (TFA)

- Password Renewal & Password Setting
- Database Consideration

From a cybersecurity perspective, the combination of the plans provided by the survey participants and the recommended actions suggested by Laulaupea'alu and Keegan is still worth utilising by the GoT. From a cultural standpoint, the inclusion of the Tongan concepts of the *hierarchal triad* and *religious belief* is significant to control OS in Tonga. The combination of all these cybersecurity features and cultural elements become strong defensive mechanisms in Tonga to fight against OS.

6.3.10 General comments on ICT development

Generally, the rapid ICT development offers enormous potential in Tonga. With the fast speed of fibre-optic cable networks, communication is easier to communicate locally and globally. Section 1.2 highlights the achievement of fibre-optic cable in 2013, which facilitates local and global communication to the government ministries, banks, businesses, churches, hospitals and citizens. One of the primary advantages of ICT is the achievement of *e-fanongonongo tokoto*, the methodology deployed by the author of this thesis to communicate and collect data from Tongan participants during COVID-19 border restrictions. The technical features of ICT development in Tonga such as fibre-optic cable, fast internet speed, availability of Zoom, Facebook, Facebook Messenger, emails, etc. assist in the achievement of this research project.

Both the technical and human features of cybersecurity have value in the overall safety of cyberspace, but this research was duly focused on the human behaviour of Tongans relates to rapid ICT development. The author of this thesis believes that human behaviour is the first step to investigate in correlation with rapid ICT vulnerabilities and then the technical features are to be carried out in a later phase. The theory of the author of this thesis is in line with the idea of Aldawood and Skinner (2018) – that cybercriminals "have focused on humans, a target considered to be the weakest link in every enterprise" (p. 62). Based on this idea, the author of this thesis decided to concentrate and investigate the vulnerabilities in the behaviour of Tongans related to rapid ICT development. The survey findings discovered the 5-core-vulnerabilities of Tongans as discussed in Section 6.3.3.

The other highlights of *e-fanongonongo tokoto* refer to the achievement and ability to answer the three main questions of the thesis. The cybersecurity vulnerabilities had been discovered and identified and greatly influenced the TIs. The cause of failure to cyberattacks and how these malicious cyber-events in Tonga exacerbated by aspects of Tongan culture have also been achieved.

CHAPTER SEVEN

7. CONCLUSION

This research has been important in its discovery of current issues affecting Tongan citizens due to rapid ICT development in Tonga. Although ICT issues were discovered by Laulaupea'alu and Keegan (2019) in 2018, these issues were only focused on technical matters. The new findings are not only limited to technical issues but extended to more in-debt issues from other disciplines. One of the highlights of the survey findings is the loss of credentials and money to cyberattacks. Cybercriminals deployed *lured baits* to phish for credentials and money from the Tongan Innocents. The loss of money and susceptability to lure baits are due to – *lack of ICT knowledge*; *greed*; *romance/love*/*empathy*; *unwillingness to report to authorities* and *lack of cybersecurity training*.

In addition, rapid ICT development has now influenced Tongan culture, Tongan language, *nofo 'a famili mo e kāinga*, (living of immediate and extended family) and the *fale 'o Ha'a Moheofo* (the house of the King). The *fale 'o Ha'a Moheofo* or the King of Tonga remains at the top of the hierarchy triad, and it is *pelepelengesi* (delicate) for Tongans to perform this immoral character. Tongans are frustrated because the *molumalu* (majestic, solemn, dignified) and *ngeia* (lordly display, dignity, honour) of the King is no longer honoured by the people.

This research has also discovered special *faito'o faka-Tonga* (Tongan remedy) to *faito'o* (treat or cure) these cybersecurity issues. Possible remedies have been uncovered in this research such as '*Tala ke i Kapa na'a ke tō ki Mala*' (Tell it while still in Kapa) (A precautionary advice of the danger ahead to be aware of), *Tahi Kulokula* (Sea of Red), *Mate ma'a Tonga* (MMT), *Tui Fakalotu* (Religious Belief), *Fakatu'utu'unga e nofo* (Hierarchal Rank). *Tahi Kulokula* and *Mate ma'a Tonga* are both common in the philosophy of *ngaue fakataha* (teamwork), *loto-taha* (to be unanimous, of one mind) *fakataha/uouongataha* (unity/solidarity), and *loto māfana* (warm heart).

Ngāue fakataha in Section 5.5.2 shows that 97% of the survey participants agreed with the idea that people together with the Government ministries could work

together to fight against OS. *Tui Fakalotu* and *Fakatu'utu'unga e nofo*, in this context, refer to the words of the *faifekau* and the message from the nobles or higher authorities to the people of Tonga. Their powerful words are potential tools to utilised by informing the people of Tonga to be aware of the consequences of ICT development.

Essential cybersecurity elements and technical features are currently deployed by the GoT but some of these features are required to be enforce and make sure they are operational. These technical features are cloud computing, penetration testing, multi-factor authentication, data encryption, data backup, cyber insurance, antivirus software, strong password, business continuity plan or incident management communication plan, and sufficient funds (budget) to purchase updated antivirus and latest software version. With the combination of these cybersecurity features and cultural practices such as *Mate ma'a Tonga*, *Tahi Kulokula*, *Tui Fakalotu*, *Fakatu'utu'unga e nofo*, *Tala ke i Kapa na'a ke tō ki Mala*, the powerful words of *faifekau* and nobles, enforcement of technical features, the author of this thesis believes the issue of OS can be mitigatd and managed within the Tongan community.

Tongan culture is a barrier to effort controlling the consequences of ICT development. Unless the true scale is provided with honesty, there is no expectation to be manageable in in fighting against OS. Without honesty it is only a reflection and dream. People are more serious about keeping the relationship, respecting, and loving the perpetrators. '*Ofa vale* (foolish love) and *'ofa poto* intelligent love should be distinguished. *'Ofa vale* is just knowing the perpetrator or not doing the right job to stop it. But giving the perpetrator a first chance to learn the first mistake. In this context, *'ofa poto* means to report the perpetrator to the right place that may lead to discipline in the lifestyle.

Succession planning is an important part of being prepared for a perfect future for our children. To effectively conclude and never blame today's parents for not doing their proper duty Addison and Taumoepeau (2016) quotes: *Ko e hakau 'o e 'aho ni, ko e fonua ia 'o e 'apongipongi* (The reefs of today will be the islands of tomorrow). The metaphoric meaning of this Tongan phrase refers to the children (*hakau*) of today who will be the *fonua* (land/Tonga/world) of tomorrow. The success of our

fānau (children) today will save Tonga ‘*apongipongi* (tomorrow). Today's parents must show and have enough power and wisdom to inform today's generation and the next generation of the problem of the ICT, to stand on their feet to deal with and overcome cybersecurity issues in the future. It is an eagle-eye’s vision, not only limited to the toe but also has a long vision to be far, long, and clear. The longer and further the vision from the toe, the greater the possibilities to save Tonga from the consequences of ICT.

Tonga is one of the leading nations of ICT development in the South Pacific. This is due to the first launch of CERT, known as Tonga CERT, the first island to achieve this imperative ICT development in 2016. Tonga became the leading nation to enact their own computer act in September 2003. Additionally, Tonga is one of the nations to connect to the Southern Cross submarine fibre-optic cable in 2013. Because of these crucial elemental facts, Tonga can say that it is one of most advanced islands in ICT development in the South Pacific. This research is relevant and beneficial for all the nations of the Pacific islands. There is no research yet on this area of cybersecurity aiming for the Pacific islands.

7.1 Research Limitations

The overall purpose of this survey is partially achieved because it is targeted to reach out to main areas in Tonga such as Government ministries, public enterprises, schools, agencies/boards, businesses, youths, consulate/embassy, churches, banks and other financial organisations. Unfortunately, the other organisations such as churches, banks and financial institutions were not able to collect data from their end. The most challenging factor encountered in this research was COVID-19 with the ban to travel overseas to meet face-to-face with the survey participants. An expectation of achieving higher numbers of survey participants but unfortunately it was not accomplished due to the travel and border restrictions. Despite the issue of COVID-19 and empty promises from the survey participants, the data collected provides sufficient information to prove that Tonga is generally influenced by rapid ICT development.

7.2 Reconsidering the thesis questions

The three main thesis questions and the answers for these questions are summarised in Chapter 6 (Discussion Chapter) but are reposted again in this section as a

conclusion. It is important to challenge whether this research addresses all the thesis questions. The conclusion of this research is the ability to answer the three main thesis questions and discovering appropriate solutions for the issues discovered in this research.

Here are the summaries of the answers for the survey questions:

Question 1: *How has rapid ICT deployment in Tonga influenced online vulnerabilities?*

Yes, there are great influences of rapid ICT development in Tonga and it is affected the people of Tonga. Scammers deployed *5-lured-baits* to entice people. Tongans failed to these baits due to *romantic, love and empathy*; *unwillingness to report online scammers to authorities*; *greed; lack of ICT knowledge* and *lack of cybersecurity training*.

Question 2: *How is the incidence of malicious cyber-events in Tonga exacerbated by aspects of Tongan culture?*

The weaknesses in Tongan cultural practices allow opportunities for the growth of OS in Tonga. The failure to report cybercriminal cases to related authorities slows down the process of fighting against OS and the tendency for controlling OS in Tonga is doubted. The failure to report cybercriminals within the Tongan community is reflected in the power of Tongan values or golden pillars. (i.e., *faka'apa'apa* (respect), *lototō* (humility), *tauhi-vā* (nurturing relationship), *'ofa* (love), and *mamahi'ime'a* (loyalty or sense of responsibility). Some of the Tongan people are stuck to the significance of Tongan values by giving them another chance rather than directly reports to related authorities.

On the other site, Tongan people are no longer pay *faka'apa'apa*, *lototō*, *tauhi-vā*, *mamahi'ime'a* and *'ofa* to the King of Tonga, nobles and other Tongans. The hierarchal rank (King, nobles and commoners) is started to *'auhia* ("to be wash away or carried along by a current" or wash away by the current of ICT. Tongan language is *fulutāmakia* ("to be suffocating or unable to breath") (Churchward, 1959) (p. 202 and 554).

Yes, the Tongan cultural practices aggravate the opportunities for OS.

Question 3: *What strategies have been identified by the research to improve ICT security in Tonga?*

Yes, there are strategic plans to improve cybersecurity vulnerabilities discovered in this research and the ICT system in Tonga. There are eleven (11) recommendations provided by Laulaupea'alu and Keegan in 2019 which are very valuable and still worth applying. Other ten (10) strategic plans were provided by the survey participants which then amalgamated with the eleven (11) recommendations to form strong plans.

Another interesting addition is the inclusion of the Tongan cultural concepts such as *Mate ma'a Tonga* (MMT), *Sea of Red* (SoR), *Tala ke i Kapa na'a ke tō ki Mala, People of God* and *Religious belief of Tongans*. All these cultural features are very powerful defensive tools to mitigate OS in Tonga. The highlight of these tools is about the religious belief of the Tongan people akin to Niumeitolu (2007), "*ko e fonua lotu 'eni" or* "…this is a Christian nation..." (p. 7). Some quotes from the participants were collected and gathered together to form one quote as mentioned below:

> '*Ko e lotu ko e mata'i-koloa 'a e Tonga. Ko e ivi mafai 'o e lotu 'i Tonga ko ha me'angaue lelei ke ta'ota'ofi'aki 'a e ngauehala'aki 'o e tekinolosia 'initaneti. Ko e ngauehala'aki 'o e tekinolosia ki ho no kakai'i e kakai ko e angahala. Ko e totongi 'o e angahala ko e mate.* [translation by author] *Lotu* (Christianity) is a foremost asset of Tongans. The power of Christianity in Tonga is a proper tool to lessen the inappropriate use of the internet technology. The misappropriate use of technology to cheat people is *angahala* (sin). The wage of *angahala* is death.

7.3 Religious belief of Tongans

[FYI; About 73% supported the idea that the words of the *faifekau* (church minister) or People of God are very powerful tools for Tonga to fight against OS (see Table 27). All of the participants (100%) believed that OS is *angahala* (sin) (see Table 28). About 84% of the survey participants believed/agreed that Christian belief in God of Tongans assists in reducing OS (see Table 29). About 90% of local Tongans are Christians as according to Niumeitolu (2007) p. 7)].

The repost of this information above is to clarify the influence of Christianity and religious belief of Tongans which is unique and powerful. The combination of all these abovementioned points clarifies the belief in God of Tongans is very strong. The influence and belief in God can assist the people of Tonga to address OS.

7.4 Recommendations

7.4.1 Cybersecurity workshops

While the purpose of this research is for diverse entities such as government ministries, boards, businesses, the researcher is concerned about the firewood level. Laulaupea'alu and Keegan (2019) quoted *Kapau kuo vela e ʻakau mataa pea huanoa e ʻakau momoa*. [translation by author] If the green trees (living trees) are fast/easy to burn, then how about the firewood (dead trees)? In this context, the green trees or living trees refer to the civil servants and educated people who use the internet and computer regularly and gain ICT experience. The firewood level refers to the computer illiterate people: the common people that are beginning to use online resources who have a lack of awareness about cybercrimes. The authors recommended that the GoT is to focus on vulnerabilities that affect the firewood as these people are the most likely to be burnt the quickest and the most by cyber-attackers. (p. 187).

To implement that idea and reach out ICT knowledge to 'firewood level', would require enough money to make it happen. The GoT must save enough budget to conduct cybersecurity workshops for all five nations in Tonga. This means, the furthermost island in Tonga, the Ongo Niua, is included in this workshop. From the survey findings, more than 95% of the survey participants agreed that conducting more cybersecurity workshops could assist in reducing OS. In addition, the voice sent from Ongo Niua to the GoT is clear on the request to have a cybersecurity workshop in their islands.

7.4.2 Deployment of cybersecurity features

After the exploitation of the ransomware attack on District Health Board Waikato in mid-May 2021, the author of this thesis visited Waikato Hospital on a personal matter. The first vehicle entry point where the Automated Parking System for issuing parking tickets was inoperative and no more automated parking tickets

issued on the entry point. This means the Parking Management Software was damaged and visitors are free to go inside and leave the hospital parking at any time free of charge. The consultation process was conducted manually with the filling of patient forms handwriting by receptionists. No patient records were able to be retrieved as computer desktops were inoperative and the doctors spent more time interviewing the patients to receive more information about the patients' histories and records.

The District Health Board Waikato computer systems were fully exploited by this ransomware attack. According to Andrew McRae, a reporter of Radio New Zealand, this ransomware attack was from overseas and cyber insurance was in place. Waikato DHB is confident that the systems must be restored without paying ransomware demanded by cyberattacks (RNZ, 2021).

The main focal point of raising this issue as there were significant factors to address in this DHB ransomware attack such as cyber insurance and data backup. Cyber insurance will be sorted out later for financial recovery of the total costs of this attack. The recovery of the patients' records is in progress and the most important point relates to the demand for the huge amount of money from the cyberattacks. The concern of the researcher is about a similar ransomware attack of this type that may occur in Tonga. The question then for Tonga is whether they can counteract and recover? There are a lot of questions to ask.

A lesson to learn from this case to ensure the cybersecurity features are in place to assist and counteract. The placement of cybersecurity features is not guaranteed to fully stop the cyberattacks but there are possibilities to assist in any sort of cyber resilience.

Laulaupea'alu and Keegan (2019) submitted eleven (11) recommendations to the GoT in 2018. Physical and electronic copies were delivered to the Prime Minister's office and various ministries and organisations. The recommendations were about cybersecurity features to be deployed to the computer systems. These features do not guarantee to fully secure the whole computer system but act as special cybersecurity layers to slow down the issues of cyberattacks. The eleven cybersecurity features are highlighted in Section 6.3.9.

The eleven (11) cybersecurity features are still valid to continue deploying by the GoT and to achieve the maximum level possible. However, there were five crucial features discovered in this research that were minor usage by the GoT. The minority usage cybersecurity features are:

- Cloud computing
- Penetration testing
- Multi-factor authentication
- Cyber insurance
- Business Continuity Plan OR Incident Management Communication Plan.

It is essential to maintain all these eleven cybersecurity features as they are crucial elements of cybersecurity. The focus aims to emphasise the last five key cybersecurity elements because it was not strong and achieved sufficient stability to be used by the GoT. The higher the number of usages, the stronger the cybersecurity level is achieved.

7.4.3 Education and overseas training

There were ten (10) strategic plans to mitigate OS in Tonga provided by the survey participants in Section 6.3.9. All these plans are very imperative to implement. Two of these plans are considered to be significant by the author of this thesis, as they are crucial for the long term cybersecurity in Tonga. These are to *include cybersecurity in the school syllabus* and to *provide education/ workshop/training*

Both of these two plans focus on education, the inclusion of cybersecurity courses in the school academic syllabus and the provision of education/workshop/training for the people of Tonga. The GoT and the Ministry of Education are to decide on providing opportunities for scholarships for students to attend cybersecurity courses overseas. The first step for the inclusion of cybersecurity in the school syllabus is to send students overseas. This new cybersecurity knowledge gained from overseas will assist in teaching cybersecurity courses that may start in secondary school.

Laulaupea'alu and Keegan (2019) recommended that:

> Tonga requires cybersecurity experts to look after the IT systems of Tonga. The primary roles of cybersecurity experts are to protect organisations from hackers. The costs associated with overseas training are small in

> comparison to the potential future cost of damage to the business or organisation. Proper training and education will empower high-quality understanding and bring advanced knowledge of security responsibilities (p. 190).

7.4.4 Suggestions for further research

Some organisations were unable to take part in this research such as banks, financial institutions and churches. There is a need to find out the impact of ICT development in these organisations. These organisations are major areas in the Tonga communities and their primary tasks are directly dealt with money.

Banks and financial institutions are the major organisations that work with money every day. Because these areas are highly sensitive, there is a need to meet and conduct a face-to-face interview. The *e-fanongonongo tokoto* (e-ft) methodology is no longer convenient. In doing the face-to-face interview, there is a potential for the survey participants to provide more information that is very hard to write the answers on the questionnaires but easily speak out. There is high expectation to collect more truthful, reliable, secret and private information from the survey participants.

In church, the monetary donation or *misinale* is the faith and belief that the proper responsibility is to donate money as a gift to God to appreciate and thank for the love that God has given to the family. *Misinale* (church donation), *fakaafe* (church feast), *li pa'anga kuata* (quarterly donation) are essential responsibilities of Tongans and it is hard to stop because it has become the basic faith of Christian to give money to God. There is a need to search for the impacts of these religious responsibilities and their relationship to OS.

7.4.5 Final Words

'Time and tide wait for no man' reminds us that human actions cannot stop the movement of the tides or the passage of time. No one is so robust as to halt the march of time or the coming of high tide, but we can make use of our time to be ready for these upcoming events. Humans are unable to stop the wave of ICT development but they can make use of time to manage the negative impacts that currently and will be occurred in the future.

Tongans need appropriate cybersecurity tools to navigate the contemporary ICT *moana* (sea). The cybersecurity tools refer to the readiness of the body, mind, and spirit. These three elements must unite and work together to achieve a healthy cyber-safe environment. The associated entities are to work together on the current crisis in Tonga today. If not all the elements work together, there will be ongoing ICT issues in the future.

ʻI Tongaʻ, ko e tui faka-Kalisitiane mo e mafai ʻo e lotuʻ ko e meʻangāue mahuʻinga ʻaupito ke pukemaʻu ke tauiʻi ʻaki e ngaahi ngāue kākā fakaemāmani lahi ʻi he Ngaluope. [translation by author] In Tonga, Christian beliefs and the power of prayers are the significant tools to hold and persistently fight against the global deception on the internet.

REFERENCES

'Ahio. (2018). *Ko e Talamalu 'o e Fonua* (3rd ed.). Tonga: Friendly Island Bookshop.

Addison, A., & Taumoepeau, S. (2016). Tourism's place in the school curriculum: a case study from Tonga'. *International Education, 1*(2), 4-28.

Advox. (2019). Tonga threatens to ban Facebook over anti-monarchy posts. Retrieved from https://advox.globalvoices.org/2019/08/20/tonga-threatens-to-ban-facebook-over-anti-monarchy-posts/

Ahmad. (2020). Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *Available at SSRN 3568830*.

Ahmad, R., & Yunos, Z. (2012). A dynamic cyber terrorism framework. *International Journal of Computer Science and Information Security, 10*(2), 149.

Akhgar, B., Staniforth, A., & Bosco, F. (2014). *Cyber crime and cyber terrorism investigator's handbook*: Syngress.

Al-Khateeb, H. M., & Epiphaniou, G. (2016). How technology can mitigate and counteract cyber-stalking and online grooming. *Computer Fraud & Security, 2016*(1), 14-18.

Aldawood, H., & Skinner, G. (2018). *Educating and raising awareness on cyber security social engineering: A literature review.* Paper presented at the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE).

Allen, B. (2018). *Knowledge and civilization*: Routledge.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69-82.

Analytica, O. (2020). Tech may curb virus profiteering, not disinformation. *Emerald Expert Briefings*(oxan-db).

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly, 34*(3), 613-643.

ANZ. (2021). Foreign exchange calculator. Retrieved from https://tools.anz.co.nz/foreign-exchange/fx-rate-calculator/

APWG. (2016). Phishing Activity Trends Report, 4th Quarter 2016. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

Aswani, S., & Graves, M. W. (1998). The Tongan maritime expansion: a case in the evolutionary ecology of social complexity. *Asian Perspectives*, 135-164.

Baker, S. W. (1897). *An English and Tongan Vocabulary: Also a Tongan and English Vocabulary, with a List of Idiomatic Phrases; and Tongan Grammar*: Wilsons and Horton.

BBC News. (2018). Tonga parliament building flattened by Cyclone Gita. Retrieved from https://www.bbc.com/news/world-asia-43039931

Bennardo, G. (2008). Metaphors, Source Domains, and Key Words in Tongan Speech about Social Relationships:'Ofa'Love'Is Giving. *Anthropological linguistics*, 174-204.

Bergholz, A., De Beer, J., Glahn, S., Moens, M.-F., Paaß, G., & Strobel, S. (2010). New filtering approaches for phishing email. *Journal of computer security, 18*(1), 7-35.

Bible in One Year. (2018). Victorious Living. Retrieved from https://www.bibleinoneyear.org/bioy/commentary/2640

Bible in One Year. (2021). Good Judgement. Retrieved from https://www.bible.com/ur/reading-plans/23472-bioy21en/day/222

Biersack, A. (1982). Tongan exchange structures: Beyond descent and alliance. *The Journal of the Polynesian Society, 91*(2), 181-212.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition. In *New Contributions in Information Systems and Technologies* (pp. 311-316): Springer.

Blanco Hache, A. C., & Ryder, N. (2011). 'Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas: 1 a critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud. *Information & Communications Technology Law, 20*(1), 35-56.

Boateng, R., Longe, O. B., Mbarika, V., Avevor, I., & Isabalija, S. R. (2010). *Cyber Crime and Criminality in Ghana: Its Forms and Implications.* Paper presented at the AMCIS.

Bourdeix, R., Johnson, V., Baudouin, L., Tuia, V. S., Kete, T., Planes, S., . . . Weise, S. (2011). Polymotu: A new concept of island-based germplasm bank based on an old Polynesian practice.

Britannica. (2019). Ha'apai Group. Retrieved from https://www.britannica.com/place/Haapai-Group

Britannica. (2020). Austronesian languages Retrieved from https://www.britannica.com/topic/Austronesian-languages

Britannica. (2021). Tonga. Retrieved from https://www.britannica.com/place/Tonga

British Library. (2018). Captain Cook and the ‘Friendly Islands'. Retrieved from https://blogs.bl.uk/untoldlives/2018/06/captain-cook-and-the-friendly-islands.html

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management, 29*(3), 408-433.

Brooks, E. B. (2017). The Resurrection of Jesus in Mark. *Alpha v1*, 81-88.

Brown. (1996). IN CHRIST. *The Sacramental Word: Incarnation, Sacrament and Poetry, London: SPCK*.

Brown. (2000). What must one believe about Jesus for salvation. *International Journal of Frontier Missions, 17*(4), 13-21.

Bryan Foltz, C. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security, 12*(2), 154-166.

Budde Communication. (2019). Tonga - Telecoms, Mobile and Broadband - Statistics and Analyses. Retrieved from https://www.budde.com.au/Research/Tonga-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses

Cambridge Dictionary. (2020). Cambridge Dictionary. Retrieved from https://dictionary.cambridge.org/

Carson. (2013). Conversation On a Train: Reflections On the Bible and Christian Discipleship‖. *Journal of European Baptist Studies, 15*, 58-70.

Cave, D. (2012). Digital islands: How the Pacific’s ICT revolution is transforming the region. *Lowy Institute for International Policy*.

CERTNZ. (2019). Scams and fraud. Retrieved from https://www.cert.govt.nz/businesses-and-individuals/explore/scams-and-fraud/?topic=scams-and-fraud

CGI Security. (2018). How do I secure my site? Retrieved from https://www.cgisecurity.com/questions/securewebsite.shtml

Chomsiri, T. (2007). *HTTPS hacking protection.* Paper presented at the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07).

Chron. (2019). Can Weather Affect Satellite Internet? Retrieved from https://smallbusiness.chron.com/can-weather-affect-satellite-internet-26822.html

Churchward, M. (Ed.) (1959). Tonga: The Government of Tonga.

Clough, J. (2014). A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation. *Monash UL Rev., 40*, 698.

Clough, J. (2015). *Principles of cybercrime*: Cambridge University Press.

Clowney, E. P. (1973). The Final Temple. *Westminster Theological Journal, 35*(2), 156-191.

Cocker J. (2013). Malo Tonga. Retrieved from http://malotonga.com/1zLeaPaloveapeVavau.html

Compelling Truth. (2019). What does it mean to be a true Christian? Retrieved from https://www.compellingtruth.org/true-Christian.html

Computer Hope. (2020). Scam. Retrieved from https://www.computerhope.com/jargon/s/scam.htm

Conklin, W. A., Shoemaker, D., & Kohnke, A. (2017). *Cyber Resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture.* Paper presented at the ICMLG 2017 5th International Conference on Management Leadership and Governance.

Consolvo S, Jung J, Greenstein B, Powledge P, Maganis G, & D, A. (2010). *The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on Wi-Fi.* Paper presented at the 12th ACM international conference on Ubiquitous computing.

Conway, M. (2011). Against cyberterrorism. *Communications of the ACM, 54*(2), 26-28.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas, 113*, 48-52.

Cox, C., & Whalen, M. (2001). On evil: an interview with Alain Badiou. *Cabinet Magazine Online, 5*, 2.

Cox, J., & Macintyre, M. (2014). C hristian Marriage, Money Scams, and M elanesian Social Imaginaries. *Oceania, 84*(2), 138-157.

Danquah, P., & Longe, O. (2011). Cyber deception and theft: An ethnographic study on cyber criminality from a ghanaian perspective. *Journal of Information Technology Impact, 11*(3), 169-182.

DBpedia. (n.p). About Tonga College. Retrieved from https://dbpedia.org/page/Tonga_College

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy, 239*, 288.

Dennis, A., Jones, R., Kildare, D., & Barclay, C. (2014). Design Science Approach to Developing and Evaluating a National Cybersecurity Framework for Jamaica. *The Electronic Journal of Information Systems in Developing Countries, 62*(1), 1-18.

Department of Justice. (2020). U.S. Attorney and IRS-CI warn taxpayers against Fraud Schemes Related to COVID-19 Economic Impact Payments. Retrieved from https://www.justice.gov/usao-sdia/pr/us-attorney-and-irs-ci-warn-taxpayers-against-fraud-schemes-related-covid-19-economic

Devpolicy. (2020). COVID-19: RSE responses, challenges and logistics. Retrieved from https://devpolicy.org/covid-19-rse-responses-challenges-and-logistics-20200415/

Digicel Tonga. (2018). Digicel launches Tonga's biggest 4G+ Network. Retrieved from https://www.digicelgroup.com/to/en/mobile/explore/other-stuff/news-community/2017/november/20th/digicel-launches-tongas-biggest-4g--network.html

Distance. (2021). Distance from New Zealand to Tonga. Retrieved from https://www.distancefromto.net/distance-from-new-zealand-to-tonga

Dixon, R. D., Levy, D. E., & Lowery, R. C. (1988). Asking the" born-again" question. *Review of Religious Research*, 33-39.

Douaire-Marsaudon, F. (1996). Neither black nor white: The father's sister in Tonga. *The Journal of the Polynesian Society, 105*(2), 139-164.

Dreamstime. (2014). St. Joseph`s Cathedral, the largest church in the town of Neiafu, Vava`u, Tonga Kingdom, Polynesia, Oceania, South Pacific Ocean. . Retrieved from https://www.dreamstime.com/st-joseph-s-cathedral-largest-church-town-neiafu-vava-u-tonga-kingdom-polynesia-oceania-south-pacific-ocean-vavau-image139386915

Edwards, W. D., Gabel, W. J., & Hosmer, F. E. (1986). On the physical death of Jesus Christ. *JAMA, 255*(11), 1455-1463.

Elliott, J. (2011). *Scammed: How to save your money and find better service in a world of schemes, swindles, and shady deals* John Wiley & Sons, Inc. .

ENotes. (2019). What are problems faced by developing countries? . Retrieved from https://www.enotes.com/homework-help/what-problems-faced-by-developing-countries-544853

Europol. (2019). Take control of your digital life. Do'nt be a victim of cyber scams. . Retrieved from https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/take-control-of-your-digital-life-don%E2%80%99t-be-victim-of-cyber-scams?fbclid=IwAR1wV7KY29M4-_FYQ9erhJKMk0oEgJlzVaP0Pn7TInEmAebobNYg9uUtj4Q

Evans, M. (1999). Is Tonga's MIRAB economy sustainable? A view from the village and a view without it. *Pacific Studies, 22*(3), 137-166.

Ezeoha. (1970). Regulating Internet Banking In Nigeria : Some Success Prescriptions- Part 2. Retrieved from https://www.icommercecentral.com/open-access/regulating-internet-banking-in-nigeria--some-success-prescriptions-part-2.php?aid=38508

Ezeoha, A. E. (2006). Regulating Internet Banking in Nigeria: some success prescriptions–part 2. *Journal of Internet Banking and Commerce, 11*(1), 35-47.

Fa’avae, D. (2020). Critical autoethnographic encounters in the moana: Wayfinding the intersections of to’utangata Tonga and indigenous

masculinities. In Wayfinding and Critical Autoethnography (pp. 69-82): Routledge.

Facebook. (2020). 'Ave Pa'anga Pau. Retrieved from https://www.facebook.com/193602281439416/posts/ave-paanga-pau-welcomes-john-vala-from-one-of-our-rse-employers-kono-motueka-mal/416319039167738/

Fairbairn-Dunlop, T. P. (2015). *Fofola e fala kae alea e kāinga: exploring the issues of communication regarding Tongan youth suicide in South Auckland, New Zealand.* Auckland University of Technology,

FAO. (2011). Migration, remittance and development Tonga. Retrieved from http://www.fao.org/3/a-an477e.pdf

FAO. (2021). FAO in Jamaica, Bahamas and Belize. Retrieved from http://www.fao.org/jamaica-bahamas-and-belize/fao-in-jamaica-bahamas-and-belize/jamaica-at-a-glance/en/

Fehoko, E. (2016). Pukepuke fonua: An exploratory study on the faikava as an identity marker for New Zealand-born Tongan males in Auckland New Zealand. In *Identity, Belonging and Human Rights: A Multi-Disciplinary Perspective* (pp. 113-124): Brill.

Ferdon, E. N. (1987). *Early Tonga: as the explorers saw it 1616-1810*: University of Arizona Press.

Fiji Sun. (2015). ATM scam exposed. Retrieved from http://fijisun.com.fj/2015/12/10/atm-scam-exposed./

Finau, G., Samuwai, J., & Prasad, A. (2013). Cyber crime and its implications to the Pacific. *The Fiji Accountant*, 15-16.

Find a Grave. (2012). George Tupou King of Tonga. Retrieved from https://www.findagrave.com/memorial/92345419/george_tupou-king_of_tonga#source

Finklea, K. M., & Theohary, C. A. (2012). *Cybercrime: conceptual issues for congress and US law enforcement*.

Finlan. (2011). Jesus in atonement theories. *Burkett (red.)*.

Fintel. (n.d.). Fiji-Vanuatu Telecommunications Cable System. Retrieved from http://www.fintel.com.fj/pages.cfm/company/news/fiji-vanuatu-telecommunications-cable-system.html

FIP Postal. (2016). Tonga tin can mail history. Retrieved from https://www.fippostalhistory.com/wp-content/uploads/2016/01/Tonga_Tin_Can_Mail-_exhibit.pdf

Florêncio, D., & Herley, C. (2007). *Evaluating a trial deployment of password re-use for phishing prevention.* Paper presented at the Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit.

Folaumoetu'i, P. (2020). Ilo h tha fka pH a Tevita Vuki. Retrieved from https://www.facebook.com/papafanifo.folaumoetui

Fox Sports. (2019). Revealed: The true dollar value of each 2017 State of Origin team. Retrieved from https://www.foxsports.com.au/nrl/state-of-origin/revealed-the-true-dollar-value-of-each-2017-state-of-origin-team/news-story/c6dda65cec5b7f3483efcfe64d397934

Francis, S. T. (2009). 13. The View from 'Home'—Transnational Movements from Three Tongan Villages. *Migration and Transnationalism*, 203.

Fruhlinger, J. (2020). What is a cyber attack? Recent examples show disturbing trends. Retrieved from https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security, 27*(7-8), 235-240.

Futter, A. (2018). 'Cyber'semantics: why we should retire the latest buzzword in security studies. *Journal of Cyber Policy, 3*(2), 201-216.

Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). *A framework for detection and measurement of phishing attacks.* Paper presented at the Proceedings of the 2007 ACM workshop on Recurring malcode.

Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in computer virology, 6*(1), 77-90.

GbMb. (2019). GB to kbit Conversion. Retrieved from https://www.gbmb.org/gb-to-kbit

Geis, G. (1991). White-collar crime: What is it? *Current issues in criminal justice, 3*(1), 9-24.

Gill, A. (2012). Memories of two kings of Tonga. *Eureka Street, 22*(5), 4.

Gillespie, A. A. (2015). *Cybercrime: key issues and debates*: Routledge.

Global Voices. (2019). Tonga threatens to ban Facebook over anti-monarchy posts Retrieved from https://advox.globalvoices.org/2019/08/20/tonga-threatens-to-ban-facebook-over-anti-monarchy-posts/

Good Reads. (2019). Foolishness to the Greeks quotes. Retrieved from https://www.goodreads.com/work/quotes/253081-foolishness-to-the-greeks-the-gospel-and-western-culture

Goodwin, C. F., & Nicholas, J. P. (2013). Developing a National Strategy for Cybersecurity. In: The Microsoft Corporation.

Gordon, & Ford. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2(1), 13-20.

Government of Tonga. (2016). PM launched Tonga National CERT. Retrieved from https://www.gov.to/press-release/pm-launched-tonga-national-cert/

Government of Tonga. (2019). Computer Crimes Bill 2019 Retrieved from https://ago.gov.to/cms/images/LEGISLATION/BILLS/2019/2019-0025/ComputerCrimesBill2019.pdf

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *IEEE Security & Privacy, 6*(1), 61-64.

Guardian. (2020). What is Covid-19? Retrieved from https://www.theguardian.com/world/2020/feb/27/what-is-covid-19

Gumble, N. (2020). Freedom. Retrieved from https://my.bible.com/en-GB/reading-plans/17704-bible-in-one-year-2020-with-nicky-gumbel/day/42

Hanley, M., Dean, T., Schroeder, W., Houy, M., Trzeciak, R. F., & Montelibano, J. (2011). *An analysis of technical observations in insider theft of intellectual property cases*. Retrieved from

Hardy, K., & Williams, G. (2014). What is 'cyberterrorism'? Computer and internet technology in legal definitions of terrorism. In *Cyberterrorism* (pp. 1-23): Springer.

Herbert, S. (2013). Literature review: poverty, social analysis and the political economy of Tonga.

Hogeveen, B. (2020). ICT for development in the Pacific islands. Retrieved from https://www.aspi.org.au/report/ict-development-pacific-islands

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81.

Internet Live Stats. (2016). Tonga Internet Users. Retrieved from https://www.internetlivestats.com/internet-users/tonga/

Internet Society. (2020). CERT Tonga first from Pacific Island Countries to become an Operational Member of APCERT. Retrieved from https://www.picisoc.org/2020/06/22/cert-tonga-first-from-pacific-island-countries-to-become-an-operational-member-of-apcert/

Interpol. (2020). Interpol warns of financial fraud linked to COVID-19. Retrieved from https://www.interpol.int/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19

Investopedia. (2021). Top 25 developed and developing countries. Retrieved from https://www.investopedia.com/updates/top-developing-countries/

Iqbal, M. (2003). Defining cyberterrorism. *J. Marshall J. Computer & Info. L., 22*, 397.

ITIF. (2019). Submarine cables: Critical infrastructure for global communications. Retrieved from http://www2.itif.org/2019-submarine-cables.pdf

James, K. (1983). Gender Relations in Tonga 1780 to 1984. *The journal of the Polynesian Society, 92*(2), 233-243.

James, K. (2002). The cost of custom: A recent funeral in Tonga. *The Journal of the Polynesian Society, 111*(3), 223-238.

James, L. (2005). *Phishing exposed*: Elsevier.

Janczewski, L. (2007). *Cyber warfare and cyber terrorism*: IGI Global.

Jayden Nowitz. (2018). An investigation into susceptibility to phishing attacks between mobile and desktop email clients (Unpublished master thesis). .

Joakim Kävrestad. (2017). What Is Cybercrime? In *Guide to Digital Forensics* (pp. 9-11): Springer.

Kaeppler, A. L. (1971). Rank in Tonga. *Ethnology, 10*(2), 174-193.

Kalavite, T. (2010). *Fononga'a fakahalafononga: Tongan students' journey to academic achievement in New Zealand tertiary education.* University of Waikato,

Kalvin Bahia. (2018). *State of mobile internet connectivity 2018*. Retrieved from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/09/State-of-Mobile-Internet-Connectivity-2018.pdf

Kaniva Tonga. (2013). Thousand assemble to mark the begining of the new Mo‘ui Fo‘ou ‘Ia Kalaisi Fellowship. Retrieved from https://kanivatonga.nz/2013/07/thousand-assemble-to-mark-the-new-fellowship-moui-foou-ia-kalaisi/

Kaniva Tonga. (2020). Tongan seasonal workers in Australia continue working as farmers around the world face shortage of labour due to Covid-19 restrictions. Retrieved from https://www.kanivatonga.nz/2020/04/tongan-seasonal-workers-in-australia-continue-working-as-farmers-around-the-world-face-shortage-of-labour-due-to-covid-19-restrictions/

Karl de Leeuw, & Jan Bergstra. (2007). *The history of information security: a comprehensive handbook*: Elsevier.

Kefu. (2011). Tonga's Cybercrime Legislation. Retrieved from https://rm.coe.int/16802f2474

Kelly Kuehn. (2019). 10 Inspirational career quotes for recent College grads. Retrieved from https://www.workitdaily.com/inspirational-career-quotes-recent-college-grads

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis*, *59*(1), 111-128.

Ketuu, O. (2014). *The Impact Of Tongan Cultural Practices On Tongans' Economic Behaviour*. ResearchSpace@ Auckland,

Kierkegaard, S. (2008). Cybering, online grooming and ageplay. *Computer Law and Security Review: The International Journal of Technology and Practice*, *24*(1), 41-55. doi:10.1016/j.clsr.2007.11.004

Koloto, A. H. a. i. (2016). Va, Tauhi Va. Retrieved from https://link.springer.com/content/pdf/10.1007%2F978-981-287-588-4_33.pdf

Kristeva, J. (1987). *In the beginning was love: Psychoanalysis and faith*: Columbia University Press New York.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847.

Kropeit, T. (2015). *Don't Trust Open Hotspots: Wi-Fi Hacker Detection and Privacy Protection via Smartphone.* Ruhr-Universitat Bochum.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*: Springer.

Kundi, G. M., Nawaz, A., Akhtar, R., & MPhil Student, I. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications, 4*(4), 61-71.

Lalitha, M. P., & Udutha, S. (2013). New Filtering Approaches for Phishing Email. *International Journal of Computer Trends and Technology (IJCTT), 4*(6), 1733-1736.

Latu, P. O. (2017). Ko E Tala-Tukufakaholo 'O Tonga: an alter-native holistic historiography of Tonga history from their own traditional oral culture and through their own people's eyes.

Latukefu. (1975). *The Tongan Constitution: A brief history to celebrate its Centenary*. Nuku'alofa, Tonga: Government Printer.

Laulaupea'alu, S. (2021). COVID-19 muddles talanoa and vā: Perceived connections and uncertainties. Waikato Journal of Education, 26, 115-123.

Laulaupea'alu, & Keegan. (2018). *Data Security Assessment for Organisations in Tonga.* Paper presented at the Cyber Forensic and Security International Conference, Nuku'alofa, Tonga.

Laulaupea'alu, S., & Keegan, T. T. A. G. (2019). Cyber security vulnerabilities in Tonga.

Le, H. (2009). Online fingerprint identification with a fast and distortion tolerant hashing. Retrieve from http://www.mirlabs.org/jias/secured/hoile.pdf

Leahy, B. (2020). Covid 19 coronavirus: Auckland man's bank card skimmed as scams on the rise. Retrieved from https://www.nzherald.co.nz/nz/covid-19-coronavirus-auckland-mans-bank-card-skimmed-as-scams-on-the-rise/5IWQ3ADHBXF73MOQJTH5EKKGKY/

Learn Tongan. (2017). Let's learn Tongan. Retrieved from https://letslearntongan.com/tongan-alphabet/

Levin, Y. (2006). Jesus,‘Son of God’and ‘Son of David’: The ‘Adoption’of Jesus into the Davidic Line. *Journal for the Study of the New Testament, 28*(4), 415-442.

Lewis. (2015). The day that never happened. Retrieved from https://nowiknow.com/the-day-that-never-happened/

Lewis, J. (1979). Volcano in Tonga. *Journal of Administration Overseas, 18*(2), 116-122.

Li, J., Zheng, R., & Chen, H. J. C. o. t. A. (2006). From fingerprint to writeprint. *49*(4), 76-82. Retrieve from https://dl.acm.org/doi/pdf/10.1145/1121949.1121951

Liu, M., Jiang, X., & Kot, A. C. (2007). Efficient fingerprint search based on database clustering. Pattern Recognition, 40(6), 1793-1803. Retrieve from https://www.sciencedirect.com/science/article/pii/S0031320306004845

Loader, B. D., & Thomas, D. (2013). *Cybercrime: Security and surveillance in the information age*: Routledge.

Local Prayers. (2012). Rev Sione Kami Memorial Church. Retrieved from https://www.localprayers.com/PG/Port-Moresby/378680548871979/Rev-Sione-Kami-Memorial-Church

Loeffler, J. (2018). No more transistors, the End of Moore’s Law. Retrieved from https://interestingengineering.com/no-more-transistors-the-end-of-moores-law

Loop Tonga. (2018). Tongan authorities investigate claim ship staff put passengers lives at risk. Retrieved from http://www.looptonga.com/tonga-news/tongan-authorities-investigate-claim-ship-staff-put-passengers-lives-risk-73023

Lu, Q., & Shi, Y. (2020). Coronavirus disease (COVID-19) and neonate: What neonatologist need to know. *Journal of medical virology, 92*(6), 564-567.

Matangi Tonga. (2014). King launches Niuafo'ou mobile network. Retrieved from https://matangitonga.to/tag/ucall-mobile-network?page=1

Moala. (n.d.). Satellite development in Tonga. Retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/Aug-ISS2017/PPT_S4_Tonga.pdf

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review, 17*, 1-24.

Mohammed, K. H., Mohammed, Y. D., & Solanke, A. A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(1), 56-63.

Morris, A. (2009). Nine a side basketball in the kingdom of Tonga: a case study in negotiating gender roles. *Transactions at play, 9*, 22.

Mow, I. T. C. (2014). Issues and challenges, strategies and recommendations, in the development of ICT in a small island developing state: the case of Samoa. *The Electronic Journal of Information Systems in Developing Countries, 63*(1), 1-24.

Nadaraja, R., & Yazdanifard, R. (2013). Social media marketing: advantages and disadvantages. Center of Southern New Hempshire University, 1-10.

Naylor, D., Finamore, A., Leontiadis, I., Grunenberger, Y., Mellia, M., Munafò, M., . . . Steenkiste, P. (2014). *The cost of the S in HTTPS.* Paper presented at the Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies.

Nisha, S., & Farik, M. (2015). Recent cybercrimes in Fiji. *International Journal of Scientific & Technology Research, 4*(8), 148-151. Retrieved from https://www.researchgate.net/publication/311714862_Recent_Cybercrimes_In_Fiji

Niumeitolu, H. T. (2007). The State and the Church, the State of the Church in Tonga.

Numbeo. (2019). Gas Prices in Nuku'alofa, Tonga. . Retrieved from https://www.numbeo.com/gas-prices/in/Nuku%27alofa-Tonga

NZ Herald. (2011). Tongan World Cup spirit eclipses rest. Retrieved from https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10749688

Oceania Exploration. (2021). How big is the Pacific Ocean? Retrieved from https://oceanexplorer.noaa.gov/facts/pacific-size.html

Ofanoa, M., Percival, T., Huggard, P., & Buetow, S. (2015). Talanga: the tongan way enquiry. *Sociology Study, 5*(4), 334-340.

Okereafor, K., & Adebola, O. (2020). TACKLING THE CYBERSECURITY IMPACTS OF THE CORONAVIRUS OUTBREAK AS A CHALLENGE TO INTERNET SAFETY. *Journal Homepage: http://ijmr. net. in, 8*(2).

Oni, A. A., & Ayo, C. K. (2010). An empirical investigation of the level of users' acceptance of e-banking in Nigeria. *Journal of Internet Banking and Commerce, 15*(1), 1-13.

Otsuka, Y. (2007). Making a case for Tongan as an endangered language. *The Contemporary Pacific, 19*(2), 446-473.

Ottis, R., & Lorents, P. (2010). *Cyberspace: Definition and implications.* Paper presented at the International Conference on Cyber Warfare and Security.

Owen, T., Noble, W., & Speed, F. C. (2017). Cyber Grooming: How Biological Variables Reinforce Cognitive Distortion. In *New Perspectives on Cybercrime* (pp. 81-111): Springer.

Palmer, T. (2008). Jesus Christ: Our ancestor? *Africa Journal of Evangelical Theology, 27*(1), 65-76.

Pandey, S., Shah, N., Sharma, A., & Farik, M. (2016). Cybersecurity Situation In Fiji. *International Journal of Scientific & Technology Research, 5*(7), 215-219.

Papacharissi, Z., & Zaks, A. (2006). Is broadband the future? An analysis of broadband technology potential and diffusion. *Telecommunications Policy, 30*(1), 64-75.

Passage. (2016). Tonga. Retrieved from http://www.svpassage.com/Tonga.htm

Pathak, P., & Nanded, Y. M. (2016). A dangerous trend of cybercrime: ransomware growing challenge. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume, 5*.

Pau'uvale, D. L. (2012). *Laulōtaha; Tongan perspectives of 'quality' in early childhood education.* Auckland University of Technology,

Petelo, S. (2017). Status of e-Government in Tonga. Retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/Sep-SCEG2017/SESSION-1_Tonga_Ms_Lesieli_Siasini_Petelo.pdf

Picclick. (2021). 1784 Cook & Webber Large 1st Edition Antique Print of Inasi Ceremony Mu'a, Tonga. Retrieved from https://picclick.com/1784-Cook-Webber-Large-1st-Edition-Antique-372978000277.html

Pink News. (2020). LGBT+ activist loses discrimination complaint against Israel Folau over infamous Instagram post claiming 'hell awaits' gay people. Retrieved from https://www.pinknews.co.uk/2020/04/22/israel-folau-garry-burns-discrimination-homophobic-instagram/

PNW. (2015). Tongan misinale celebrates financial giving. Retrieved from https://www.pnwumc.org/news/tongan-misinale-celebrates-financial-giving/

Pollitt, M. M. (2002). Cyberterrorism-Fact or Fancy. *Focus on Terrorism, 9*, 65-69.

Prescott, S. M., & Hooper, K. C. (2009). Commons and anti-commons: Tongan business experiences in New Zealand. *Pacific Accounting Review, 21*(3), 286-303.

Pultarova, T. (2016). Webcam hack shows vulnerability of connected devices. *Engineering & Technology, 11*(11), 10-10.

Rabone, S. (1845). *A Vocabulary of the Tonga Language: Arranged in Alphabetical Order: to which is Annexed a List of Idiomatical Phrases*: Wesleyan Mission Press.

Rachinger, M., Rauter, R., Müller, C., Vorraber, W., & Schirgi, E. (2019). Digitalization and its influence on business model innovation. *Journal of Manufacturing Technology Management*.

Ravulo, J. (2015). Pacific communities in Australia. Retrieve from https://ro.uow.edu.au/cgi/viewcontent.cgi?article=4901&context=sspapers

Rennie, S. J. (1991). Subsistence agriculture versus cash cropping—the social repercussions. *Journal of rural studies, 7*(1-2), 5-9.

Research Gate. (2021). Life cycle of phishing attack. Retrieved from https://www.researchgate.net/figure/Life-cycle-of-phishing-attack-2_fig1_342050858

Return Path. (2019). What is a Cloudmark fingerprint and how does it work? Retrieved from https://help.returnpath.com/hc/en-us/articles/220564147-What-is-a-Cloudmark-fingerprint-and-how-does-it-work-

Richards, N. (1988). Is humility a virtue? American Philosophical Quarterly, 25(3), 253-259.

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review, 13*(1), 10-21.

RNZ. (2016). Tonga looks at laws to curb cyber crime. Retrieved from https://www.rnz.co.nz/international/pacific-news/314739/tonga-looks-at-laws-to-curb-cyber-crime

RNZ. (2018). Hawaiki cable lands in American Samoa. Retrieved from https://www.rnz.co.nz/international/pacific-news/355828/hawaiki-cable-lands-in-american-samoa

RNZ. (2019a). Tevita Pangai Jr turns down NSW, commits to Tonga. Retrieved from https://www.rnz.co.nz/international/pacific-news/389771/sport-tevita-pangai-jr-turns-down-nsw-commits-to-tonga

RNZ. (2019b). Tonga officials meeting Facebook in Aust over attacks. Retrieved from https://www.rnz.co.nz/international/pacific-news/398464/tonga-officials-meeting-facebook-in-aust-over-attacks

RNZ. (2020). Cook Islands submarine fibreoptic cable to go live in May. Retrieved from https://www.rnz.co.nz/news/pacific/407086/cook-islands-submarine-fibreoptic-cable-to-go-live-in-may

RNZ. (2021). Waikato DHB confident it can restore computer system without paying ransom. Retrieved from https://www.rnz.co.nz/news/national/443147/waikato-dhb-confident-it-can-restore-computer-system-without-paying-ransom

Ropelato, J. (2006). Internet pornography statistics. Retrieve from http://ministryoftruth.me.uk/wp-content/uploads/2014/03/IFR2013.pdf

Saberi, A., Vahidi, M., & Bidgoli, B. M. (2007). *Learn to detect phishing scams using learning and ensemble? methods.* Paper presented at the Proceedings of the 2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology-Workshops.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security, 56*, 70-82.

Saini, H., Rao, Y. S., & Panda, T. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications, 2*(2), 202-209.

Schaeffer, F. A., & Kennedy, D. J. (1981). A Christian manifesto (pp. 17-18). Westchester, IL: Crossway Books. Retrieve from https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=508c429b512b4e2a99ad2082bdaaecfb352b7f63

Schaper, M. T., & Weber, P. (2012). Understanding small business scams. *Journal of Enterprising Culture, 20*(03), 333-356.

Scott, N. (2007). Cyber Legislation: A model law for the South Pacific. Retrieved from https://www.wgtn.ac.nz/law/research/publications/about-nzacl/publications/special-issues/hors-serie-volume-ix,-2009/Scott.pdf

Segal, A. (2013). The code not taken: China, the United States, and the future of cyber espionage. *Bulletin of the Atomic Scientists, 69*(5), 38-45.

Seib, P., & Janbek, D. M. (2010). *Global terrorism and new media: The post-Al Qaeda generation*: Routledge.

Senthilkumar, N., Gitanjali, J., Monika, A., & Monisha, R. (2020). Fraudulence Detection and Recommendation of Trusted Websites. In *Emerging Research in Data Engineering Systems and Computer Communications* (pp. 413-425): Springer.

Shadden, B. (2005). Aphasia as identity theft: Theory and practice. *Aphasiology, 19*(3-5), 211-223.

Shover, N., Hochstetler, A., & Alalehto, T. (2013). Choosing white-collar crime. In *The Oxford handbook of criminological theory* (pp. 475-493): Oxford University Press Oxford.

Siegel, R. K. (1980). The psychology of life after death. *American Psychologist, 35*(10), 911.

Society. (2020). A Cook's tour of Tonga. Retrieved from https://www.captaincooksociety.com/home/detail/a-cook-s-tour-of-tonga

Statista. (2021). Loss through cyber crime in the United States in 2020. Retrieved from https://www.statista.com/statistics/234993/us-states-with-the-largest-losses-through-cybercrime/

Statistics Department. (2010). Household income and Expenditure Survey Retrieved from http://prism.spc.int/images/documents/HEIS/2009_Tonga_HIES_Report_Final.pdf

Statistics Department. (2014). Tonga 2011 census of population and housing, Volume 2: Analytical Report. Retrieved from https://tonga.prism.spc.int/component/advlisting/?view=download&fileId=302&Itemid=301

Stuff. (2017). Jason Taumalolo says it will be hard to walk away from Tonga as fellow defectors look to stay put. Retrieved from https://www.stuff.co.nz/sport/league/99249117/jason-taumalolo-says-it-will-be-hard-to-walk-away-from-tonga-as-fellow-defectors-look-to-stay-put

Stuff. (2019a). Israel Folau rejected a A$1 million payout offer. Retrieved from https://www.stuff.co.nz/sport/rugby/international/112472840/israel-folau-rejected-a-1-million-payout-offer--report

Stuff. (2019b). The pros and cons of Tonga becoming a tier one rugby league nation. Retrieved from https://www.stuff.co.nz/sport/league/113599145/the-pros-and-cons-of-tonga-becoming-a-tier-one-rugby-league-nation

Swartz, N. (2007). Protecting information from insiders. *Information Management, 41*(3), 20.

Symantec Corporation. (2003). Cyberterrorism. Retrieved from https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

Tafea, M. K. (1999). The Tongan Pentecost of 1834. A revival in the kingdom of Tonga: A possible key for renewal and unity for the Tongan church today. Asbury Theological Seminary.

Talakeikapa. (2018). The journey begins. Retrieved from https://talakeikapa18.wordpress.com/2018/09/03/the-journey-begins/

Tamanikaiwaimaro, S. (2010). *Cyber Security in the Republic of Fiji.* Paper presented at the Internet Governance Forum, Diplo Foundation. Retrieved from http://www. diplomacy. edu/resources/general/cyber security-republic-fiji.

Tangata Pasifika. (2020). Online scams targeting Pacific people. Retrieved from https://tpplus.co.nz/community/online-scams-targeting-pacific-people/

Tankard, C. (2018). Tackling push payment scams. *Network Security, 2018*(1), 20. doi:https://doi.org/10.1016/S1353-4858(18)30009-6

Taumoefolau, M. (2013). 7 Respect, Solidarity, and Resilience in Pacific Worldviews. *Pacific identities and well-being: cross-cultural perspectives*, 115.

TeAra. (2015). Tongans by Melenaite Taumoefolau. Retrieved from https://teara.govt.nz/en/tongans/print

Techtarget. (2021). Dictionary attack. Retrieved from https://searchsecurity.techtarget.com/definition/dictionary-attack

Tecun, A. (2017). Tongan kava: Performance, adaptation, and identity in diaspora. *Performance of the Real E-journal, 1*(1), 52-64.

Teisina. (2011). Semantic Scholar . Retrieved from Langa ngāue 'a e kau faiako Akoteu Tonga nofo 'i Aotearoa.: https://www.semanticscholar.org/paper/Langa-ng%C4%81ue-'a-e-kau-faiako-Akoteu-Tonga-nofo-'i-Teisina/720c7a75f9ce1177d9232b13b918ccd5fc3c679a

Tekstas. (n.d.). Motivation: types and reasons. Retrieved from http://uki.vdu.lt/wp-content/uploads/sinergija/EN/geografija/geografija3/Tekstas%20Migration,%20%20%C4%AFvadinis%20pratimas.pdf

Tevita, O. (2005). Tauhi va: Nurturing Tongan sociospatial ties in Maui and beyond. *The Contemporary Pacific, 17*(1), 83-114.

The Kingdom. (2018). The South Pacific's Only Monarchy. Retrieved from https://thekingdomoftonga.com/the-kingdom-today/

The University of Waikato. (2017). Government of Tonga and Waikato cyber security collaboration. Retrieved from http://www.waikato.ac.nz/news-events/media/2017/government-of-tonga-and-waikato-cyber-security-collaboration

The World Bank. (2013a). Connecting Tonga through Broadband Internet. Retrieved from

https://www.worldbank.org/en/news/feature/2013/12/10/connecting-tonga-through-broadband-internet

The World Bank. (2013b). High Speed Broadband Goes Live in Tonga. Retrieved from https://www.worldbank.org/en/news/press-release/2013/08/21/high-speed-broadband-goes-live-in-tonga

The World Bank. (2020). The World Bank in Middle Income Countries. Retrieved from https://www.worldbank.org/en/country/mic/overview

Thompson, D. W., & Thompson, D. A. W. (1942). On growth and form (Vol. 2, p. 470). Cambridge: Cambridge university press.

Thompson Memorials. (2015). Pacific Island Shipping Services. Retrieved from https://www.thompsonmemorials.co.nz/Services/Pacific+Island+Shipping+Service.html

Tofuaipangai, S., & Camilleri, P. (2016). Social policy, social work and fatongia: Implications of the Tongan concept of obligation. *Aotearoa New Zealand Social Work, 28*(1), 60-67.

Tonga Broadcasting Commission. (2018a). Fibre optic cable launched in Vava'u. Retrieved from http://www.tonga-broadcasting.net/?p=11133

Tonga Broadcasting Commission. (2018b). Tonga earns multi-million dollars from seasonal workers program. Retrieved from http://www.tonga-broadcasting.net/?p=12933

Tonga Broadcasting Commission. (2019). New e-government projects to be implemented in the next fiscal year. Retrieved from http://www.tonga-broadcasting.net/?p=14962

Tonga Department of Statistics. (2014). Tonga 2011 Census of Population and Housing, Volume 2: Analytical Report. Retrieved from https://tonga.prism.spc.int/component/advlisting/?view=download&fileId=302&Itemid=301

Tonga Development Bank. (2016). 'Ave Pa'anga Pau. Retrieved from https://www.avepaanga.co.nz/

Trading Economics. (2019a). Samoa GDP. Retrieved from https://tradingeconomics.com/samoa/gdp

Trading Economics. (2019b). Samoa GDP Per Capita PPP. Retrieved from https://tradingeconomics.com/samoa/gdp-per-capita-ppp

Trading Economics. (2019c). Tonga GDP. Retrieved from https://tradingeconomics.com/tonga/gdp

Trading Economics. (2019d). Tonga GDP Per Capita PPP. Retrieved from https://tradingeconomics.com/tonga/gdp-per-capita-ppp

Travel Guide. (2020). Tonga: the Friendly islands of Captain Cook. Retrieved from https://www.travelguide-en.org/tonga/#

Travel Guideline. (2011). Tonga: A Polynesian Paradise. Retrieved from https://www.travelguideline.net/tonga-a-polynesian-paradise.html

Trend Micro. (2018). Ransomware. Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/Ransomware

Tropina, T. (2016). Do Digital Technologies Facilitate Illicit Financial Flows? *Background paper for the World Development Report*.

Tu'inukuafe. (1992). *A simplfied dictionary of modern Tongan*: Polynesian Press.

Tu'ipulotu, S. T. T. (2013). *Gospel of hope for the world of hopeless: The success of early Christianity and hope for the Tongan Church*: Claremont School of Theology.

Turner, J. W. (1986). " The Water of Life": Kava Ritual and the Logic of Sacrifice. *Ethnology*, *25*(3), 203-214.

TVNZ. (2019). Tongan advisory council hit out at 'exploitation' of fans after Kiwis Test. Retrieved from https://www.tvnz.co.nz/one-news/sport/league/tongan-advisory-council-hit-exploitation-fans-after-kiwis-test

UCG. (2004). What Is a True Christian? Retrieved from https://www.ucg.org/the-good-news/what-is-a-true-christian

Unicef. (2020). *Key Messages and Actions for COVID-19 Prevention and Control in Schools*. Retrieved from https://www.who.int/docs/default-source/coronaviruse/key-messages-and-actions-for-covid-19-prevention-and-control-in-schools-march-2020.pdf?sfvrsn=baf81d52_4

Unilang. (2019). Tongan for beginners. Retrieved from https://unilang.org/course.php?res=81

United Nations. (2014). Country classification. Retrieved from https://www.un.org/en/development/desa/policy/wesp/wesp_current/2014wesp_country_classification.pdf

Vadera, A. K., & Aguilera, R. V. (2015). The evolution of vocabularies and its relation to investigation of white-collar crimes: An institutional work perspective. *Journal of Business Ethics, 128*(1), 21-38.

Vaioleti, T. M. (2006). Talanoa research methodology: A developing position on Pacific research. *Waikato Journal of Education, 12*.

Vaka'uta, N. (2009). TĀLANGA: Theorizing a Tongan mode of interpretation. *AlterNative: An International Journal of Indigenous Peoples, 5*(1), 126-139.

Volkamer, M., Renaud, K., & Gerber, P. (2016). Spot the phish by checking the pruned URL. *Information & Computer Security*.

Wallsten, S. (2005). Regulation and internet use in developing countries. *Economic Development and Cultural Change, 53*(2), 501-523.

White House. (2018). National Cyber Strategy of the United States of America. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Whitsett, C. G. (2000). Son of God, Seed of David: Paul's messianic exegesis in Romans 2: 3-4. *Journal of Biblical Literature, 119*(4), 661-681.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking, 15*(3), 181-183.

Wikipedia. (2021). Tongan funerals. Retrieved from https://en.wikipedia.org/wiki/Tongan_funerals

Willison, R., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM, 52*(9), 133-137.

World Atlas. (2019). International Date Line Retrieved from https://www.worldatlas.com/aatlas/infopage/dateline.htm

World Atlas. (2021). Maps of Tonga. Retrieved from https://www.worldatlas.com/maps/tonga

World Bank Group. (2020). Closing the digital divide in Tonga. Retrieved from https://www.worldbank.org/en/results/2019/09/16/closing-the-digital-divide-in-tonga

World Health Organization. (2020). Rolling updates on coronavirus disease (COVID-19). Retrieved from https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen

World Meter. (2021). Coronavirus. Retrieved from https://www.worldometers.info/coronavirus/country/new-zealand/

World Meter. (2020). Tonga Population. Retrieved from https://www.worldometers.info/world-population/tonga-population/

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407-427.

Yi, Y., Lagniton, P. N., Ye, S., Li, E., & Xu, R.-H. (2020). COVID-19: what has been learned and to be learned about the novel coronavirus disease. *International journal of biological sciences, 16*(10), 1753.

Yoon, C. (2010). Antecedents of customer satisfaction with online banking in China: The effects of experience. *Computers in Human Behavior, 26*(6), 1296-1304.

ZDNet. (2019). Tonga signs 15-year satellite deal after January cable outage. Retrieved from https://www.zdnet.com/article/tonga-signs-15-year-satellite-deal-after-january-cable-outage/

Zhang, Y., Hong, J. I., & Cranor, L. F. (2007). *Cantina: a content-based approach to detecting phishing web sites.* Paper presented at the Proceedings of the 16th international conference on World Wide Web.

APPENDIXES

Appendix 1: Special Acknowledgement

This endeavour would not have been possible without the assistance of special people from several islands in Tonga. These people are honoured and named Good Samaritans. Overall, about six (6) GSs contributed, a lot to making this research happen. There were 3 GSs in Tongatapu, 2 GSs in Vava‘u, and 1 GS in Niuatoputapu.

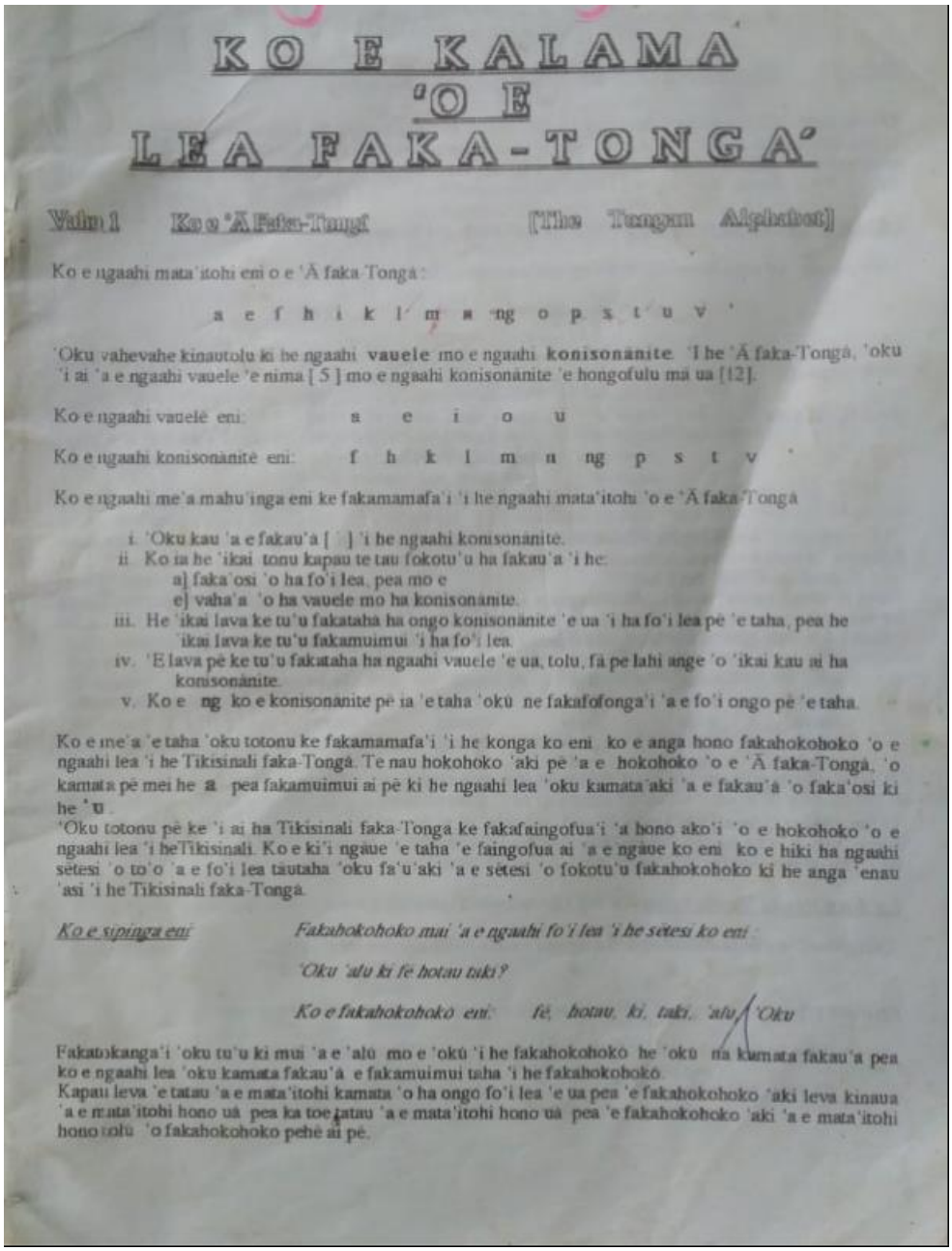
They assisted in delivering the questionnaires to the survey participants through various methods such as emails and hard copies. The highlights of their works were the printing out of hard copies and delivery to the participants. All expenses involved were paid with the GSs’ own money. The return of the answered hard copies to New Zealand through Air New Zealand was also paid for by theses GSs.

Words cannot express my gratitude to honour your good works. Without your hardworking, willingness, *faka‘apa‘apa, lototō, tauhi-vā, ‘ofa, and mamahi‘ime‘a*, this research is not achieved.

God Bless and *Mālō ‘aupito.*

Appendix 2: Vowel and consonant in Section 2.5.2

The image below is a screenshot of a secondary school lecture note named '***Ko e Kalama 'o e Lea Faka-Tonga***'. It is the first page of the lecture note that was photographed by a Primarily Teacher in Tonga and sent to the author of the thesis via Facebook Messenger to confirm where the original information came from. There is no online information about this secondary school lecture note.



KO E KALAMA
'O E
LEA FAKA-TONGA'

Vahe 1 Ko e 'Ā Faka-Tongá [The Tongan Alphabet]

Ko e ngaahi mata'itohi eni o e 'Ā faka-Tonga:

a e f h i k l m n ng o p s t u v '

'Oku vahevahe kinautolu ki he ngaahi **vauele** mo e ngaahi **konisonānite**. 'I he 'Ā faka-Tongá, 'oku 'i ai 'a e ngaahi vauele 'e nima [5] mo e ngaahi konisonānite 'e hongofulu mā ua [12].

Ko e ngaahi vauelē eni: a e i o u

Ko e ngaahi konisonānitē eni: f h k l m n ng p s t v '

Ko e ngaahi me'a mahu'inga eni ke fakamamafa'i 'i he ngaahi mata'itohi 'o e 'Ā faka-Tongá

i. 'Oku kau 'a e fakau'a [ ] 'i he ngaahi konisonānitē.
ii. Ko ia he 'ikai tonu kapau te tau fokotu'u ha fakau'a 'i he:
a] faka'osi 'o ha fo'i lea, pea mo e
e] vaha'a 'o ha vauele mo ha konisonānite.
iii. He 'ikai lava ke tu'u fakataha ha ongo konisonānite 'e ua 'i ha fo'i lea pē 'e taha, pea he 'ikai lava ke tu'u fakamuimui 'i ha fo'i lea.
iv. 'E lava pē ke tu'u fakataha ha ngaahi vauele 'e ua, tolu, fā pe lahi ange 'o 'ikai kau ai ha konisonānite.
v. Ko e **ng** ko e konisonānite pē ia 'e taha 'okú ne fakafofonga'i 'a e fo'i ongo pē 'e taha.

Ko e me'a 'e taha 'oku totonu ke fakamamafa'i 'i he konga ko eni ko e anga hono fakahokohoko 'o e ngaahi lea 'i he Tikisinali faka-Tongá. Te nau hokohoko 'aki pē 'a e hokohoko 'o e 'Ā faka-Tongá, 'o kamata pē mei he **a** pea fakamuimui ai pē ki he ngaahi lea 'oku kamata'aki 'a e fakau'á 'o faka'osi ki he **'u**.
'Oku totonu pē ke 'i ai ha Tikisinali faka-Tonga ke fakafaingofua'i 'a hono ako'i 'o e hokohoko 'o e ngaahi lea 'i heTikisinali. Ko e ki'i ngaue 'e taha 'e faingofua ai 'a e ngāue ko eni ko e hiki ha ngaahi sētesi 'o to'o 'a e fo'i lea tāutaha 'oku fa'u'aki 'a e sētesi 'o fokotu'u fakahokohoko ki he anga 'enau 'asi 'i he Tikisinali faka-Tongá.

Ko e sipinga eni *Fakahokohoko mai 'a e ngaahi fo'i lea 'i he sētesi ko eni:*

'Oku 'alu ki fē hotau tuki?

Ko e fakahokohoko eni: *fē, hotau, ki, tuki, 'alu, 'Oku*

Fakatokanga'i 'oku tu'u ki mui 'a e 'alú mo e 'okú 'i he fakahokohokó he 'okú na kamata fakau'a pea ko e ngaahi lea 'oku kamata fakau'á e fakamuimui taha 'i he fakahokohokó.
Kapau leva 'e tatau 'a e mata'itohi kamata 'o ha ongo fo'i lea 'e ua pea 'e fakahokohoko 'aki leva kinaua 'a e mata'itohi hono uá pea ka toe tatau 'a e mata'itohi hono uá pea 'e fakahokohoko 'aki 'a e mata'itohi hono tolú 'o fakahokohoko pehē ai pē.

Appendix 3: Participants' answers in Section 5.2.4

- I can't exactly remember how I ended up on a website where I was chatting on an online pop-up chat to someone from that website. All I can remember is there was an ad about making money online through some software or online system that was simple. It intrigued me as a student to earn money while I was at university and after asking questions to whoever I was speaking to and looking at all the testimonials of how much people around the world are making and a few phone calls in place, I fell to the tricks of their ad and clicked on a payment plan using my credit card details and made a payment. As soon as the payment went through, the pop-up chat disappeared, and I tried to contact the person by email, but they never responded back. The phone number they called was also not connected and the call could not get through.

- '*I he 'asi fakatu'upakee hake 'a e virus warning 'i he'eku desktop komipiuta na 'e fiema'u leva ke u kumi 'a e antivirus-software pe na'e suggest mai ke totongi mo install ka na'e 'osiange 'aho 'e taha ne maumau 'e ku computer*. [translation by author] A virus warning promptly popped up on my computer desktop, which suggested buying an antivirus-software. The scammer suggested purchasing and installing the software and the next day I realised my computer was no longer working.'

- *Koe'uhi ko e tokotaha na'a ne fai e ngaue kaka ni ko e tokotaha 'Initia ia, ko u pehee ko e haa hono 'aonga 'e te lipooti (ki he ka u Polisi). Ko e 'Initia ia na'a ne fai e me'a pea si'isi'i ha'aku tui 'e lava 'e he kau polisi 'i Tonga ni 'o fai ha me'a ki ai*. [translation by author] Because the person who did this fraud is an Indian, I think there is no use in reporting it to the police. It was the Indian who did this scam and I have little faith that the Tongan police can do anything about it.

- *Na'a ne ne talamai 'oku 'i ai 'ene account lauimiliona 'ihe pangike, 'oku ne fiema'u kema joint venture, pea te ne 'omai 'eku pa'anga mei he bank.* [translation by author] The scammer adviced that he owned multimillion account in the bank, and he needed a joint account venture and that hewill give me money.

- I was working on my laptop with a wireless connection. Suddenly, a pop-up message came up on my screen saying the laptop is freezing and saying there's a virus providing a toll-free number to call. Indeed, the mouse didn't work or maybe I panicked and never realized that my screen was working. But I panicked and called the toll-free number because I thought there was a virus.
- They (scammers) send me a link to fill in and provide my number. I received a phone call and they asked for my bank details….. They tried to access my bank account and stole my available balance.
- My case was brought to court and the magistrate himself clearly explained the things that needed to be brought (exhibit) etc. for evidence…. I was at the site about an interesting book and when I was about to download it, it asked for my bank account information. As a result of this loss, the victim also reported that can't sleep well at night; can't focus well at work; and is tired most of the time during working hours.
- An unknown number texted me to my Nokia mobile phone and told me that I won a Samsung raffle with the grand prize of £200,000.00. The amount of money is ready to be paid out. I started to get greedy by this amount of money because if I can get it, this amount will be triple in my currency. But because I never enter any Samsung raffle that is where I suspected something is not right. The next day the unknown number called me, and the voice was a male voice. He told me if I needed my prize money, I had to send them USD 10,000.00 for deposit and clearance so they would be able to send my prize. I know this is not true and this person is trying to trick me get money from me. In my case, I was laughing because I got the scammer red-handed, but I do understand it would be a different feeling if I was sending the USD 10,000.00, they want to clear my grand prize of £200,000.00.
- *Na`e fetu`utaki mai `ae fika muli ki heeku telefoni `o talamai koe kautaha tila me`alele nautolu `oku nau tu`uaki atu `ae ngaahi me`alele `ihe mahuinga matu`aki ma`ama`a aupito. Pea talamai ke `oange eku email kene send mai kiai ae ngaahi details `oe ngaahi me`alele pea `ikai keu ave `e au kau tamate`i atu `e au `ae telefoni.* [translation by author] A foreign contact phoned on my phone and told me that the manufacturer of the vehicles advertised at extremely

affordable prices. And tell me to give my email so he sent me the details of vehicles but I did not give it to them and hung up the phone.

- *Ko e product na'e tu'uaki mai ko e laptop… pea ne fiema'u mai ke 'oange 'eku fakamatala pangike ka e toki lava fakatau e product ko 'eni.* [translation by author] The product advertised as a laptop... and the scammer wanted to give my bank statement so that this product could be purchased.

- '*Na'e 'iai pe 'eku fakakaukau 'oku mo'oni 'e ni pea taha ne fu'u fiema'u 'aupito ha me'alele ke fefononga'aki e famili…. Na'e totongi mai he'eku aunty ki he tokotaha ni (scammer), pea 'ikai 'ilo pe na'e anga fefe 'e ne ngaue 'o 'ikai ma'u e me'alele. Ko e hoko atu ai pe 'e ku suffer he 'alu ki he ako, pea 'ikai ha me'alele ke fononga holo ai e famili … Hoha'a koe'uhi ko e pa'anga ne mole, he 'oku 'ikai ke 'iai ha ngaue lelei ka ko e folau he toli fuai'i 'akau*. [translation by author] It was all in my mind that the proposed arrangement for purchasing a vehicle was true as we needed a family vehicle.... My aunty paid the money to a person (scammer) and did not know how it was going on as the vehicle was not yet received. As a result, a continuous suffer with no transportation to school and no vehicle for family transportation…. Worried because of the money lost as no fixed income for the family but a family member travelled overseas to pick fruit to purchase a family vehicle.

- The scammer asked for my bank account information…... As a result, I can't sleep well at night, can't focus well at work, and am tired most of the time during working hours.

- ….. an important process of transferring money, transactions show a suspicious account to which the money is being transferred to, and the owner of this suspicious account had a similar ID as mine but it was fake and duplicated.' The victim also advised that this scam was reported to the MoP and the bank. While they (MoP and bank) were still in the process of investigating, the victim also mentioned that: 'I was not supposed to use any of my internet access devices for a few days.

- They tricked me with stories that I already heard of it, also providing stories like they are *faka'ofa* (feelings of love or sympathy) and they need my help. I was

so emotional when they told me their sad stories. Some emailed me stories of their achievement and they needed my assistance in doing their work so they will provide me financially….. I was so mad when I went and did my shopping and the cashier told me that my card was rejected. I didn't check my card right away because I had cash with me at the time. When I reached home, I went straight to the bank and checked my account and found out there was no money. I discussed with my husband a way forward to deal with at the time, decreasing our budget and less spending until we have more cash inflows.

- *Ne fakahoko eni he email pea mo e telefoni… fiemau ke fakahu mai e pa'anga ki he account… ko e fees ia ki he ngaue 'oku fai kae malave ke transfer atu e pa'anga monu'ia…ko e pa'anga ko eni ne faka'ali koe pa'anga lahi aupito ….* [translation by author] Contacts made from scammer by email and telephone … required to deposit money to account… it about fees for the service that must be paid before releasing the lucky-money … the amount they showed is a huge amount of money.

- I thought it was my fault for believing in what the scammer was asking of me to do. They asked for an initial payment to buy a system that will allow me to make money fast and I believed them. I should have been wiser.

Appendix 4: Participants' answers in Section 5.2.8

- The scammers used names that sound familiar to me and some stories of what they achieved. It is like they know you well and I thought the person I'm talking to is family or relatives.
- I wanted their advertised product.
- I like the person, and the person kept sending me romantic emails and songs, that's good enough for me to trust that person that I have no idea who he was.'
- *Na'aku ma'u ha e-mail mei he tokotaha mei Congo ko 'ene talamai 'oku 'iai 'ene pa'anga 'oku loto kema vahevahe he 'oku 'ikai kene falala ki ha taha ka ko au pe koe $ 300000 us koe me'a na'ane kole mai keu deposit ange $ 250 us ki he 'ene account kae lava ke transfer mai e pa'anga kiate au….. Na'ane kole mai koe vave ange 'eku sent ange pa'anga koe vave ange ia 'ene transfer mai pa'anga ki he'eku account…… Na'ane 'ohovale 'i he'eku talaange ki ai 'oku ou 'ilo'i lelei pe 'ene me'a 'oku fiema'u pea 'oku ne feinga ke kakaa'i au..Na'ane tamate'i mai leva 'ene telefoni pea mo 'ene e-mail.* [translation by author] I received an e-mail from a person from Congo telling me he has US$ 300,000 and needed to share with me because he doesn't trust anyone. He asked me to deposit US$ 250 into his account so the money could be transferred to me….He told me the sooner I sent the money the faster the transfer of money to my account…. He was surprised when I told her I knew well about his plan and what he was trying to deceive me.. He then turned off his phone and his e-mail.
- They sent me a friend request and I accepted, and they sent me a friendly greeting and that is how we became friends on FB and they try to show us they want to share with us a big amount of money and they want our account to send them, so they can transfer it to our account.
- The use of good explanations, for example, giving them my personal information for a chance to live and get a good job in America, Canada, and the UK.
- They said that I won money and to receive the money, I need to send them money first.
- *Me'a malie he na'aku fakafonu pe ngaahi me'a ne nau fiema'u mai. Pea ko 'ene a'u pe ki he 'eke mai 'eku fika account he bank, pea 'ikai teu tali 'e au ha me'a*

pea fiu nautolu he toe feinga mai. Kae ʻikai pe teu toe tali. [translation by author] Fortunately, I filled out their needs. And when my bank account number was asked, I did not answer anything, and they tried several contacts with me. But I never answered.

Appendix 5: Participants' answers in Section 5.2.12

- Currently, NOT all the people of Tonga are aware of cybercrime. Education, workshops, and all other means of disseminations MUST apply. Such as newspapers, radio, television, ads on Facebook and YouTube, billboards beside the road, put in the secondary schools' curriculum at least it reaches to elders and youths to have the same understanding.
- In my view, the numbers of online businesses are increasing these days and since many Tongans are new with the new technology, it is very much needed to conduct workshops and training, so people are familiar and know how to protect themselves from these scammers. These scammers are very smart and know how to trick people especially when it comes to money. They sweet talk about all the benefits they will get when joining then end up requesting personal information as a way for them to steal money from.
- '*Oku ou tui pe 'oku mahu'inga pe ke ako e kakai Tonga ke nau 'ilo'i e ngaahi palopalema kuo hoko he ngaahi 'aho ni he ko hono 'uhinga kuo hake mai e fakalakalaka pea lahi mo e ngaue'aki e ngaahi naunau fakatekinolosia 'i Tonga ni. 'Oku 'i ai pe e totonu ke ako'i e fanau mo e kakai he sosaieti ke nau 'ilo ki hono malu'i kinautolu mei he kau kaka*. [translation by author] I just think it is important for Tongan people to learn about the problems that have been happening these days because development has come up and there has been a lot of use of technology in Tonga. Children and people in society have a right to be taught to know about protecting themselves from fraudulent actors.
- Almost all our computer users in Tonga are not cybercrime literate, they need a readiness program.
- Online scamming awareness and education should be raised more in the Kingdom because almost everyone has access to the internet now and online purchasing is increasing such as vehicle online purchasing is becoming more common now. Workshops, education could prevent people in the Kingdom from falling easily to online scammers.
- Tongan people lack knowledge in protecting themselves from online scams. It is vital to educate them on how to avoid being an online scam victim.

- We in developing countries sometimes fall into these traps very easily, especially if they are saying that you have awarded or won a large amount of money. In this case, people need to educate more on scammers.
- Many Tongan people had already spoken to me about different online incidences where they too fell for the bait of scammers. I also had also my spouse nearly believe that someone was going to offer him money after making an initial payment to someone speaking (writing) from the screen. My husband nearly fell into the same mistake I made. Luckily, he was very scared to make any deposits of money, and this served him well.
- '*Oku ou tui malohi ke teke mo ako'i e kakai hotau fonua kenau tokanga mo faka'ehi'ehi hono ngaue'aki moe taimi 'oku hu mai ai 'ae kakai kakaa ni kene uesia kinautolu. Pea 'oua na'a to ngofua foki kiha pa'anga pe manumanu 'e ma'u ai kae tokanga mo faka'eke'eke kiha taha ke tokoni atu telia na'a kakaa'i koe ha kakai*. [translation by author] I strongly believe in pushing and teaching the people of our country to be vigilant and avoid using and when these deviation people come in to ruin them. And don't be easily beaten up with money or greed that will find it but be careful and ask someone to help you to avoid deceiving you.
- *Fakahoko ha ngaahi polokalama kihe community felave`i pea moe palopalema ni ke ilo he kakai oe fonua oku malava pe ke hoko ae faingataa ni kiate kinautolu kapau e ikai kef ai ha tokanga ki ai*. [translation by author] Implement a series of community-related programs and this problem to let the people of the country know that this challenge is possible for them if it doesn't get any attention.
- Since Tonga moved on to E-Government, the government must develop the legal framework and the insights of the local, for example, if ever Tongans use Mobile for internet payment, etc. locals must be trained on the technologies, etc.
- Most of the old age are unaware of the different forms of scamming at the same time they tend to use social media to communicate with relatives overseas. The trend of using social media is very high in Tonga for both old and high school students and there are lots of online businesses as well. People of Tonga should be educated about scamming to avoid being scammed.

- A lot of Tongan people do not take this issue very seriously unless they got scammed and learned from it. The more education/workshops will provide a clear understanding and alert people about online scamming.
- Yes, as people are vulnerable since they are increasingly using the Internet. Scammers are professional and know how to provide attractive invitations.
- Internet service is a new thing to us. Our knowledge of it is inadequate. Because of this everyone is so excited to be part of it. This is a dilemma for us as people who scam know that we are easy to target.
- People need to learn more about technology and how it's affected your life if you use it in a bad manner. And to know how to avoid those scammers from happening. And treat it as serious issues as we need to be aware.
- *Kiate au oku mahu'inga aupito ke nau ilo pea lava ke nau faka'ehi'ehi mei ha nau fetaulaki mo ha palopalema pehe. Ke mahino kiate kinautolu oku malava ke kaka'i kinautolu 'o mole ai ha'a nau pa'anga*. [translation by author] To me it's very important that they know and be able to avoid encountering such a problem. To understand that it's possible to manipulate them and lose them money.
- *Fiema`u ke educate `ae kakai `oe fonua fekau`aki moe issue ko eni koe`uhi ko `etau masiva `oku tau vulnerable ange tautolu koe`uhi ko etau to ngofua kiha tu`uaki mai ha ngaahi koloa ma`ama'a he ngaluope*. [translation by author] We need to educate the citizens about this issue because of our poverty we are more vulnerable therefore we are easily down to advertising cheap goods on the internet.

Appendix 6: Approval from Tonga

MINISTRY OF METEOROLOGY,
ENERGY, INFORMATION, DISASTER
MANAGEMENT, ENVIRONMENT,
CLIMATE CHANGE AND
COMMUNICATIONS (MEIDECC)
NUKU'ALOFA, TONGA

Ref: Cps 32/2/1/19

Mr. Siuta Laulaupea'alu
8 Joanna Place
Deanwell
Hamilton 3206
New Zealand

February 1st 2019

Re: Request to Reschedule Research and survey in the Government Ministries in Tonga

Dear Siuta.

I do hope that all is well. This letter serves to advice you that the research deferment you have requested towards your PHD thesis *"The vulnerability to Online Scamming in contemporary Tongan Society* "has been duly approved to start on the 2nd April 2019 and will end on 2nd October 2019.

We look forward for the outcome of your research will be of great benefit to the Government as the results will inform Government on issues relating to online scamming and assist in devising a way forward to addressing and mitigating it's impact. And to provide a safe and secure digital environment for the people and organisations of Tonga.

We wish you all the best on this endeavour.

Yours Sincerely

MINISTRY OF METEOROLOGY, ENERGY, INFORMATION DISASTER MANAGEMENT, ENVIRONMENT CLIMATE CHANGE & COMMUNICATIONS
MEIDECC TONGA

Paula P. Ma'u
Chief Executive Officer for MEIDECC

P.O.Box 1380, Nuku'alofa, TONGA: Tel (676) 28 170: Fax (676) 24 861: Email: enquiries@mic.gov.to: URL: www.gov.to/forum/mic.gov.to

Appendix 7: Ethic Approval from the University of Waikato

Faculty of Computing and Mathematical Sciences
Rorohiko me ngā Pūtaiao Pāngarau
The University of Waikato
Private Bag 3105
Hamilton
New Zealand

Phone +64 7 838 4322
www.cms.waikato.ac.nz

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

1st May 2018

Siuta Laulaupea'alu
C/- Department of Computer Science
THE UNIVERSITY OF WAIKATO

Dear Siuata

Application for approval under the Ethical Conduct in Human Research and Related Activities Regulations

I have considered your application to conduct a research project "The vulnerability to Online Scamming in contemporary Tongan Society" with permission from the Tongan Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications & Climate Change (MEIDEC) as stated in their letter of 10th April 2018.

The procedures provided in your request are acceptable however please ensure that the Managers/Line Managers have also given signed consent for their staff to participate.

I note that participants involved in the study will not be identified in any resulting publications or the reports, and that at the conclusion of the project the data will be submitted to the FCMS Data Archive for secure storage for five years.

The Participant Information Sheet, Research Consent Form and questionnaire comply with the requirements of the University's human research ethics policies and procedures.

I therefore approve your application to perform the research project.

Mike Mayo
Human Research Ethics Committee
Faculty of Computing and Mathematical Sciences

Appendix 8: Letter to survey participants

8 Joanna Place
Deanwell
Hamilton 3206
New Zealand
Email: sl258@students.waikato.ac.ns
Email: siutalau@gmail.com
Mob: (+64) 02108129435

'Alaa si'oku kainga Tonga,

Ref: The vulnerability to Online Scamming in contemporary Tongan society

Maloo e lelei,

You are invited to participate in a research study titled "***The vulnerability to Online Scamming in contemporary Tongan society***". This study is being conducted by Siuta Laulaupea'alu from the Department of Computer Science at the University of Waikato, Hamilton, New Zealand. This research is to investigate the understanding and knowledge of the Tongan people about Online Scamming. It is my concern about the fast-growth of cybercrime includes Online Scamming and the people of Tonga are affected by this global issues. The results of this research will help to develop sustainable strategies in Tonga to mitigate risks associated with this international issue.

In this study, you will be asked to complete an electronic survey. Your participation in this study is voluntary and you are free to withdraw your participation from this study at any time. The survey should take only 30 minutes to complete.

This survey has been approved by the University of Waikato and the Government of Tonga. There are no risks associated with participating in this study. The survey collects no identifying information of any respondent. All of the responses in the survey will be recorded anonymously.

While you will not experience any direct benefits from participation, information collected in this study may benefit the Government of Tonga in the future by better understanding the cybersecurity weaknesses in Tonga.

If you have any questions regarding the survey or this research project in general, please contact Siuta Laulaupea'alu or my primary supervisor Associate Professor Te Taka Keegan at Mob: (+64) 021321315 or tetaka.keegan@waikato.ac.nz.

By completing and submitting this survey, you are indicating your consent to participate in the study.

Your participation is appreciated.

SLaulaupea'alu

Siuta Laulaupea'alu
Doctoral Candidate
Department of Computer Science
University of Waikato
Hamilton
New Zealand

Appendix 9: Consent Form

ID Number: ……..

Research Consent Form

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Ethics Committee, Faculty of Computing and Mathematical Sciences

The Vulnerability to Online Scamming in contemporary Tongan Society.

Consent Form for Participants

I have read the **Participant Information Sheet** for this study and have had the details of the study explained to me. My questions about the study have been answered to my satisfaction, and I understand that I may ask further questions at any time.

I also understand that I am free to withdraw from the study before ***Monday 31st December 2020***, or to decline to answer any particular questions in the study. I understand I can withdraw any information I have provided up until the researcher has commenced analysis on my data. I agree to provide information to the researchers under the conditions of confidentiality set out on the **Participant Information Sheet**.

I agree to participate in this study under the conditions set out in the **Participant Information Sheet**.

Signed: _____

Name: _____

Date: _____

Researcher's Name and contact information:

Siuta Laulaupea'alu Email: sl258@students.waikato.ac.nz

Supervisor's Name and contact information: (if applicable)

Associate Professor Te Taka Keegan Email: tetaka@waikato.ac.nz
Associate Professor David Nichols Email: daven@waikato.ac.nz
Dr. Vimal Kumar Email: vimal.kumar@waikato.ac.nz

Appendix 10: Survey Questions to GoT and People

ID Number: ……

Interview Questions

Section A: Demographic

(Please circle the right answer and fill in the space provided)

1. What is your gender?

Female ☐ Male ☐

2. How old are you?

A. Below 16 years
B. 16 – 20 years
C. 21 – 30 years
D. 31 – 40 years
E. 41 – 50 years
F. 51 – 60 years
G. 61 – 70 years
H. Above 70 years

3. Are you married?

A. Yes
B. No
C. Divorce

4. Which region do you come from?

A. Tongatapu
B. Vava'u
C. Ha'apai
D. Ongo Niua
E. 'Eua
F. Other, Please specify - _____

5. Please write in the space below, the name of your village?

_____

6. Which organisation do you belong to?

A. Government Ministry
B. Public Enterprise
C. Bank
D. School
E. Church
F. Individual
G. Consulate/Embassy
H. Agency/Body
I. AID Agency
J. Youth
K. Other, please specify _____.

7. What device(s) do you use to access the internet? (More than one answer is applicable)

A. Mobile
B. Computer Desktop
C. Laptop
D. Tablet
E. Mobile device for inward/outward call only without connection to internet
F. Only use traditional home line phone to make inward/outward call
G. Never use any device
H. Other, Please specify - _____

8. What is your main source of income?

A. Farm
B. Fishing
C. Weaving
D. Carving
E. Wages/salary from the Government
F. Overseas remittance from children/family(s)
G. Other, please specify

_____

9. How much do you earn annually?

A. Less than T$1,000
B. T$1,001 - T$4,000
C. T$4,001 - T$7,000
D. T$7,001 - T$10,000
E. T$10,001 - T$40,000
F. T$40,001 - T$70,000
G. T$70,001 - T$100,000
H. More than T$100,000
I. More than T$1,000,000

10. What sort of qualification have you attained?

A. No Qualification
B. Certificate in _____ from _____University/Institute
C. Diploma in _____from _____University/Institute
D. Bachelor of _____from _____University/Institute
E. Master of _____from _____University/Institute
F. Doctorate of _____from _____University/Institute
G. Other, please specify _____

11. Do you agree to continue the interview?

A. Yes
B. No
C. Not sure

12. If you answered 'No' to the above question, would you like me to come back again another time to continue the interview?

A. Yes
B. No
C. Not sure

13. If you answer 'No' to the above question, please explain the main reason(s)

_____

_____

_____

_____

_____

Section B: Cybersecurity Questions

14. Have you ever been a victim of online scamming? (E.g. phishing emails, fake antivirus software, fake websites, credit card, lottery scams etc.)

A. Yes
B. No
C. Not sure

15. Do you know anyone else who has been a victim of online scamming?

A. Yes
B. No
C. Not sure

16. How many times have you been a victim of online scamming?

A. None B. One

C. Two
D. Three
E. More than Three
F. Other, please specify _____

17. Did you lose any money?

Yes ☐ No ☐

18. How much money was lost?

A. Under $100
B. $100-$1,000
C. $1,001-$5,000
D. $5,001-$10,000
E. $10,001-$50,000
F. $50,001-$100,000
G. more than $100,000

19. What time did the online scamming take place?

A. No sure
B. Morning (12.00 midnight – 6.00 am)
C. During the day (6 am – 12.00 midday)
D. Afternoon (12.01 pm – 6.00 pm)
E. Evening (6.01 pm – 12.00 midnight)
F. Not sure
G. Other, please specify _____

20. What year did the online scamming happen?

A. Before 1990
B. 1990 – 1999
C. 2000 – 2004
D. 2005 – 2009
E. 2010 – 2014
F. 2015 – 2018
G. Not remembered

Other, please specify _____

21. Did you report this scam to the Ministry of Police or other related authorities?

Yes ☐ No ☐

22. If your answer to the above question is 'No', please explain why you did not report it?

_____

23. Was the Ministry of Police or other related authority able to solve this issue?

Yes ☐ No ☐

24. If you answered 'Yes' to the above question, please explain how the Ministry of Police or other related authority solved this issue.

_____

_____

_____

_____

_____

25. If you answered 'No' to the above question, please explain why this issue is unsolved.

_____

_____

_____

_____

_____

26. What is your strategic plan to solve similar issues in the future? Please explain your answer.

_____

_____

_____

_____

27. How did they (scammers) contact you?

A. Received a text through mobile
B. Received a phone call from an unknown person
C. An email/contact was sent to me from my friend
D. A new email/contact was sent to me from an unknown person
E. My friend phone and sent me a link to open
F. Other, Please specify _____

_____

28. What sort of information did the scammer ask for?

A. No information required

B. Bank Information: account number, username, password, credit card, etc.

C. Personal details: Name, address, date of birth, IRD number, security number, etc.

D. Asked to answer questions in a survey, open an attachment in an email, and click a website link.

E. Asked for the names of people, friends, relatives, family members, etc.

F. Other, Please specify _____

_____

_____

29. Have you given your secret information to the scammer?

A. Yes

B. No

C. No sure

30. Please explain why you gave your secret information to the scammer.

_____

_____

_____

_____

_____

31. Please explain clearly what happened and how the scammers tricked you?

_____

_____

_____

_____

32. Please explain clearly the effects (health issue and family issue) when you were caught by the scammers.

_____

_____

_____

33. Please explain clearly your feelings (e.g. stress, anxiety) when you were caught by the scammers.

_____

_____

_____

_____

_____

34. Do you learn from your error/mistake?

Yes ☐ No ☐

35. Do you think there will be a similar case in the future?

Yes ☐ No ☐

36. Please explain what you learnt from your error/mistake?

_____

_____

_____

_____

_____

37. Did any member of the family/friend/community know you were scammed?

Yes ☐ No ☐

38. Please explain how these people knew that you were scammed.

_____

_____

_____

_____

39. Please explain clearly the reactions from your family, community and friends when they discovered that you were caught by scammers.

_____

40. Are the reactions from these people helpful or not? Please explain.

_____

_____

_____

_____

41. Do you have a plan to protect yourself from scammers?

Yes ☐ No ☐

42. Please explain your plan to protect you from scammers?

_____

_____

_____

_____

43. Do you think Tongan people need education or more workshops to assist in protecting themselves from the scammers?

A. Yes B. No C. No sure

44. Please explain the reason for your answer?

_____

_____

_____

_____

45. Did the Government of Tonga or any organisation conduct any Cybersecurity workshop/training?

Yes ☐ No ☐

46. Did you enrol in this workshop?

A. Yes

B. No

C. Not Sure

47. How many times have you enrolled in this Cybersecurity workshop/training?

A. No attendance
B. One
C. Two three
D. Four
E. More than 4
F. Other, please specify _____.

48. Was the workshop useful/helpful to you?

Yes ☐ No ☐

49. How was it useful/helpful to you?

_____

_____

_____

_____

50. Is there a cybersecurity expert in your organisation?

Yes ☐ No ☐

51. What qualification does your organisation's cybersecurity expert hold?

H. No Qualification
I. Certificate in _____ from _____ University
J. Diploma in _____from _____ University
K. Bachelor of _____from _____ University
L. Master of _____from _____ University
M. Doctorate of _____from _____ University
N. Other, please specify _____.

52. Do you/your organisation think Cybersecurity workshops/training will assist to protect Tonga from cybercrimes?

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

53. Are you/your organisation planning to conduct workshops/training in the future?

Yes ☐ No ☐

54. If the Government of Tonga decides to install another satellite network connection to standby for the existing submarine fibre optical cable. Any stage where any unintentional breakdown of network communication than the satellite network will take responsibilities. Do you agree with this idea?

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

55. From cybercriminal perspective, do you think the propose satellite network will assist in reducing or speed up cybercriminal? (Please circle/tick the right answer)

A. reducing cybercriminal
B. speed up cybercriminal
C. no idea about this question

56. Please give your reasons for your choice above.

_____

_____

_____

_____

_____

Section C. General Question

Please show your answer to the following questions by ticking/circling the applicable number in the boxes below

	Remarks	Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree
57.	Internal isolation of Tonga is a major issue for ICT (Information Communication Technology) development	1	2	3	4	5
58.	Do you think the location and exposure of Tonga to hurricane and cyclone hinder the growth of ICT development?	1	2	3	4	5
59.	Cyber resilience helps to speed up ICT recover after Cyclone Gita destructed Tonga in 2018	1	2	3	4	5

60.	Judges in Tonga require cybersecurity knowledge to assist in judging cybercriminals	1	2	3	4	5
61.	Insider threats already existed within some organisations in Tonga	1	2	3	4	5
62.	Home Based Internet Users are more likely to victimise by online scammers due to the absence of other supports and limited knowledge of ICT	1	2	3	4	5
63.	Do you think that cyberbullies existed in Tonga now?	1	2	3	4	5
64.	Cyber-grooming is about building an emotional relationship with a child to gain trust aiming for exploitation or sexual abuse. Does cyber-grooming exist in Tonga?	1	2	3	4	5

If you answer more comments to support your answers above please explain in the spaces provided below the reason(s) for your answers.

_____

_____

_____

Section D. More Cybersecurity

Please tick/circle the right answer (yes or no) from the table below.

	Questions	Yes	No
65.	Did you/your organisation set up a strong password (e.g. combination numbers, letters, symbols (@,#,$,%,!,~,&,*), both uppercase and lowercase, and at least six characters) on your computer system		
66.	Did you/your organisation install antivirus software to protect from viruses and malicious programs?		
67.	Did you/your organisation update software and your computer to the latest version?		
68.	Did you/your organisation back up your data regularly?		

69.	Did you/your organisation use Cloud Computing Technology to store your data/information?		
70.	Did you/your organisation use firewall to protect your computer system?		
71.	Did you/your organisation use multi-factor authentication to access to your data/information?		
72.	Did you/your organisation use Data Encryption to secure your sensitive information/data?		
73.	Did you/your organisation carried out Penetration Testing to test for loopholes on your websites?		
74.	Did you/your organisation deploy Cyber Insurance to protect your information and cover loss in the time of physical/natural disaster?		
75.	Did you/your organisation hire any Cyber Security Expert to check the overall safety of your computer system?		
76.	Did you/your organisation deploy any Business Continuity Plan OR Incident Management Communication Plan?		
77.	Did you/your organisation provide sufficient funds (budget) to purchase updated antivirus and latest software version?		

78. If you answer "NO" to one of these questions above, please explain in the spaces provided below the reason(s) for your answers.

_____

_____

Section E. Preventative Aspects

Please show your answer (agreement or disagreement) to the following questions by ticking/circling the applicable number in the boxes below

	Prevention	Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree
79.	To conduct more cybersecurity workshops could assist to reduce Online Scamming	1	2	3	4	5
80.	To develop ICT policy at the workplace could assist to reduce Online Scamming	1	2	3	4	5

81.	Training and updating the ICT knowledge of people assist to reduce Online Scamming	1	2	3	4	5
82.	To send students oversea for further studies on cybersecurity will bring new knowledge to assist Tonga	1	2	3	4	5
83.	Government of Tonga is to consider planning to include some basic training on cybersecurity in the Government Secondary School level	1	2	3	4	5
84.	To hire Cyber Security Experts will assist Tonga to identify cybersecurity vulnerabilities	1	2	3	4	5
85.	People of Tonga, the Government ministries and organisations could work together to fight against Online Scamming	1	2	3	4	5
86.	Do not reply to any email sent to you from an unknown sender or someone you do not know	1	2	3	4	5
87.	Open an email from an unknown sender confirms your email address is alive and open an opportunity for the senders to respond back make further offers	1	2	3	4	5
88.	If you are suspicious of any contact, it is safer to do a further search about the contacted senders	1	2	3	4	5
89.	If you are suspicious of websites it is good to seek assistance from other people include ICT experts	1	2	3	4	5
90.	Security Policy, management, and other Policies are effective tools to be deployed	1	2	3	4	5

Section F. Final Report

91. Do you think this research is important for Tonga?

Yes ☐ No ☐

92. If you answered NO to the above question, please explain why this research is not important to Tonga.

Reason(s):_____

_____

_____

93. Please explain the current issue(s) or previous problem(s) that occurred within this organisation in regard to online scamming.

_____

_____

_____

What are the plans to overcome these issues?

_____

_____

_____

Now that we have finished this interview and you have answered these questions, do you think you are more aware of possible scams?

Yes ☐ No ☐

- How do you think your behaviour will change because of this interview?

Please explain

_____

_____

_____

Appendix 11: Cyber-grooming Questions

ID Number ……..

Cyber-grooming Questions

A. DEMOGRAPHIC QUESTIONS

1. What is your gender?

Male ☐ Female ☐

2. How old are you?

A. Below 16 years
B. 16 – 20 years
C. 21 – 30 years
D. 31 – 40 years
E. 41 – 50 years
F. 51 – 60 years
G. 61 – 70 years
H. Above 70 years

3. Are you married?

A. Yes B. No C. Divorce

4. Where do you come from?

A. Tongatapu
B. Vava'u
C. Ha'apai
D. Ongo Niua
E. 'Eua
F. Other, Please specify - _____

5. What computer device(s) do you use to access to the internet? (Allow more than one answer)

A. Mobile
B. Computer Desktop
C. Laptop
D. Tablet
E. Mobile device for inward/outward call only without connection to internet
F. Only use traditional home line phone to make inward/outward call
G. Never use any device
H. Other, Please specify - _____

6. What is the main source of your income?

A. Farm
B. Fishing
C. Weaving
D. Carving
E. Wages/salary from the Government
F. Overseas remittance from children/family(s)
G. Other, Please specify _____

7. What is your annual income?

A. Less than T$1,000
B. T$1,001 - T$4,000
C. T$4,001 - T$7,000
D. T$7,001 - T$10,000
E. T$10,001 - T$40,000
F. T$40,001 - T$70,000
G. T$70,001 - T$100,000
H. Over than T$100,000
I. Over than T$1,000,000

B. INCOMING FRIEND REQUEST

(***These questions relate to incoming request from outside internet users to request a friendship to the Tongans***)

8. Have you ever been contacted by someone through the internet and requested to you for friendship?

A. Yes
B. No

9. What type of media device that this person contacted you?

A. Facebook
B. Facebook Messenger
H. Twitter
I. Email
J. Instagram
K. Snapchat
L. LinkedIn
M. YouTube
N. Other, Please specify _____

10. Did you accept the incoming request for friendship?

A. Yes
B. No

11. Why did you accept or not accept this incoming request (Please explain)

_____

_____

12. Did you know this person before?

A. Yes
B. No

13. Did you discuss about the future of your friendship? (E.g. marriage or to meet face to face)

A. Yes
B. No

14. How long is your friendship?

Please give the year(s) _____

15. Is your friend(s) local or overseas?

A. Local B. Overseas C. Not Sure

16. Did you meet face to face with your friend(s)?

A. Yes B. No

17. What is the future plan of your friendship? (Please explain).

_____

_____

18. Did you experience any issue(s) with your friendship?

A. Yes B. No

19. If you answer 'Yes' to the above question, please explain the major issue(s)

_____

_____

20. Is your friendship still continue?

A. Yes B. No

21. If you answer 'No' to the above question, please explain your reason(s)

_____

_____

22. Is there any stage that your friend(s) ask something from you (like money) to assist him?

A. Yes B. No

23. Did you accept and give what your friend(s) ask?

A. Yes B. No

24. Please explain the reason(s) why you accept or not accept the request from your friend?

_____

_____

25. If you accept and give item(s) or money to your friend(s), please give detail of the item(s), value of the item(s) or amount of money that you give to your friend(s).

Type of item(s): _____ Value of item(s): _____

Amount of Money: _____

26. How did you sent the item(s) or money to your friend (Please describe)

_____

27. Any stage that your friend(s) contacted and frightened you through internet?

A. Yes B. No

28. If you answer 'Yes' to the above question, please explain how and why your friend contacted and frightened you?

_____

_____

_____

29. Did you report to the police or related authority?

A. Yes B. No

30. If you answer 'No' to the above question, please explain why you did not report it?

_____

_____

_____

31. Did the police or related authority able to solve or unsolved your problem? (Please explain the outcome)

_____

_____

_____

32. Please explain the general condition of your friendship?

_____

_____

_____

C. OUTGOING FRIEND REQUEST

(***These questions relate to outgoing request from Tongan individuals to request friendship to outside internet users***)

33. Have you ever been contacted to someone through the internet and requested for friendship?

A. Yes B. No

34. What type of media devices) that you used to contact this person? (Allow more than one answer)

A. Facebook
B. Facebook Messenger
C. Twitter
D. Email
E. Instagram
F. Snapchat
G. LinkedIn
H. YouTube
I. Other, Please specify _____

35. Did you use your real name, address, and other true identity to confirm you are true person?

A. Yes B. No

36. If you answer 'No' to the above question, please explain why you are not giving your true identity?

_____

_____

37. Did your request for real friendship or other reasons? (e.g. fake and personal gain)

A. Yes B. No

38. If you answer 'No", please explain the main reason(s) of your friendship request?

_____

_____

39. Did your request for friendship accept by the outside individual(s)?

A. Yes B. No

40. If you answer 'Yes', please explain why your outgoing request accepted?

_____

_____

41. Please give the number(s) of your Online friend(s)

Number(s) _____

42. Did you know this person(s) before?

C. Yes D. No

43. Did you arrange/discuss about the future of your friendship? (E.g. marriage or to meet face to face)

C. Yes D. No

44. How long is your friendship?

Please give the year(s) _____

45. Is your friend(s) local or overseas?

D. Local E. Overseas F. Not Sure

46. Have you meet face to face with your friend(s)?

C. Yes D. No

47. What is the long term plan of your friendship? (Please explain).

_____

_____

_____

48. Did you experience any issue(s) with your friendship?

C. Yes D. No

49. If you answer 'Yes' to the above question, please explain what is the major issue(s)

_____

_____

_____

50. Is your friendship still continue?

C. Yes D. No

51. If you answer 'No' to the above question, please explain what happened?

_____

_____

_____

52. Is there any stage that you asked something from your friend(s) (like money) to assist you?

C. Yes D. No

53. If you answer 'Yes' to the above question, please give detail of the item(s), value of the item(s) or amount of money that you received from your friend(s).

Type of item(s): _____ Value of item(s): _____

Amount of Money: _____

54. How did your friend sent the item or money to you (Please describe)

_____

_____

55. Is there any stage that you received your item(s) or money from your friend(s) and then deny to make any more contact with your friend(s)?

A. Yes B. No

56. If you answer 'Yes', please explain the main reason(s) for denying to make further contact with your friend(s)

_____

_____

_____

57. Please explain the overall condition of your friendship?

_____

_____

_____

Appendix 12: Cultural Questions

ID Number ……

Ngaahi Fehu'i

Konga A. Ngaahi Fehu'i Fakaikiiki

1. Ko e ha fa'ahinga 'oku ke kau ki ai?

Tangata ☐ Fefine ☐

2. *Ko e haa ho ta'u motu'a?*

A. Si'i he ta'u 16
B. Ta'u 16 – 20
C. Ta'u 21 – 30
D. Ta'u 31 – 40
E. Ta'u 41 – 50
F. Ta'u 51 – 60
G. Ta'u 61 – 70
H. 'Ove he ta'u 70

3. 'Oku ke mali?

A. 'Io
B. 'Ikai
C. Mavae

4. *'Oku ke ha'u me i fee?*

A. Tongatapu
B. Vava'u
C. Ha'apai
D. Ongo Niua
E. 'Eua
F. Makehe, Kataki fakamahino'i - _____

5. Kataki 'o tohi 'i lalo 'a e hingoa e feitu'u 'oku ke ha'u me i ai?

_____

6. *Ko e fee fa'ahinga kulupu 'oku ke kau ki ai?*

A. Potungaue 'a e Pule'anga
B. Public Enterprise
C. Pangike
D. Ako
E. Lotu
F. Tokotaha pe
G. Consulate/Embassy
H. Agency/Body
I. AID Agency
J. To'utupu
K. Other, please specify _____.

7. *Ko e haa e me'angaue faka-komipiuta 'oku ke ngaue'aki ki ho'o ngaue faka-'Initanetii)(Malava pe ke lahiange ho'o tali)*

A. Telefoni To'oto'o
B. Computer Desktop
C. Laptop
D. Tablet
E. Telefoni to'oto'o ke tali mo taa telefoni ka 'oku 'ikai ngaue'aki e 'initaneti
F. Laini Telefoni 'i 'api ke tali e ngaahi taa telefoni mai mo taa telefoni ki tu'a
G. 'Ikai ke ngaue'aki ha fa'ahinga me'angaue
H. Ngaahi me'angaue makehe, kataki fakamatala'i - _____

8. *Ko e ha ho'o ma'u'anga mo'ui?*
A. Ngoue
B. Toutai
C. Lalanga
D. Ngaue Fakamea'a
E. Vahenga me i he Pule'anga
F. Tokoni me i muli e fanau mo e famili
G. Ngaahi ma'u'anga mo'ui makehe (Kataki fakamatala angee)

---

9. Ko e ha e lahi e pa'anga 'oku ke ma'u he ta'u?
A. Si'isi'i hifo he T$1,000
B. T$1,001 - T$4,000
C. T$4,001 - T$7,000
A. T$7,001 - T$10,000
A. T$10,001 - T$40,000
A. T$40,001 - T$70,000
A. T$70,001 - T$100,000
B. 'Ova he T$100,000
A. 'Ova he T$1,000,000

10. Ko e ha ho tu'unga faka-Ako?
A. 'Ikai ha tu'unga faka-Ako
B. Certificate in _____ from _____ University
C. Diploma in _____from _____ University
D. Bachelor of _____from _____ University
E. Master of _____from _____ University
F. Doctorate of _____from _____ University
G. Other, please specify _____

11. Ko e ha ho tu'unga faka-Ako?
Kuo ke 'osi fetaulaki pe ma'u ko e ha fa'ahinga ngaue kakaa pe ngaue 'o e ngaluope?

A. ‘Io

B. ‘Ikai

C. ‘Ikai fakapapaui’i

12. ‘Oku ke loto ke hoko atu e faka’eke’eke?

A. Yes

B. No

C. Not sure

13. Oku ke loto ke u to e foki mai ha taimi ke he ke hoko atu e faka’eke’eke?

A. Yes

B. No

C. Not sure

14. Kapau ‘oku ke tali ‘’Ikai’ ki he fehu’i ‘olunga, kataki fakamatala’i e ‘uhinga ki ho’o tali

_____

_____

_____

_____

_____

Konga B. Ngaahi Fehu’i fekau’aki mo e ‘ulungaanga ‘o e Tonga

Ko e ngaahi fehu’i ni ‘oku fakatefito ia he ngaahi ‘ulungaanga faka-Tonga hangē ko e ngaahi **kavei koula ‘a e Tonga** (***faka’apa’apa, tauhi-vā, mamahi’ime’a, lototō mo e ‘ofa***) pe a mo e ngaahi makatu’unga makehe ‘i he nofo ‘a e Tonga. ‘Oku fakataumu’a ‘a e ngaahi fekumi ni ke ‘ilo’i pe ‘e ‘i ai ha fehokotaki ‘o e ‘ulungaanga faka-Tonga mo e ngaahi ngaue ‘a e Tonga ki he ngaahi ta’au fakamamani lahi ‘o e tekinolosia faka-Komipiuta mo e ngaahi ngaue ‘oku ‘ikai totonu ‘oku lolotonga hoko he Ngaluope. ‘E hoko nai ‘a e ngaahi ‘ulungaanga faka-Tonga ko e tokoni ke fakasi’isi’i pe ‘e hoko ia ko ha ngaahi makatu’unga ke mafola vave ange ai ‘a e ngaue ‘oku ‘ikai totonu hangee ko ha no faka-e-haua e totonu ‘a e tangata he’ene ngaue’aki ‘e ne totonu ki he Ngaluope pe ‘Initaneti.

Ki a kinautolu ‘oku kau mai ki he savea ni, kataki ‘o fili ho’o tali pe a fokotu’u ki ai e faka’ilonga ni (✓) ‘i he puha pea tohi e tali he ngaahi laini ‘oku ‘atā ‘i laloo.

A. Paloveape Faka-Tonga

Ko e fakakaukau ‘o e Palōveape faka-Tonga, ‘***Tala ke i Kapa na’a ke tō ki Mala’***, ‘oku fakataumu’a ki he kakai Tonga ke tokateu ki he ngaahi palopalema ‘oka hoko mai he kaha’u. Taimi pe ‘e hoko mai e palopalema ‘oku ‘osi fai pe teuteu ki ai. Ko e fakakaukau ko ia he palōveape ni ‘oku ne takiekina kitautolu Tonga ke tau to e mateuteuange ki he ngaahi ta’au ‘o e fakalakalaka faka-Tekinolosia ‘o e ‘Initanetii he kuo kamata ke haa ‘a e ngaahi ola-tamaki ki he fonua he taimi ni, hangee ko e ‘asi e faihia ngaue’aki e tekinolosia faka-Komipiuta.

15. *“Oku ke tui ki he fakakaukau ‘o e **‘Tala ke i Kapa na’a ke tō ki Mala’** (tokateu ki he faingata‘a he kaha‘u) ‘e malava ke ngaue‘aki ke tau mateuteu na‘a tau too ki ha faingata‘a he kaha‘u fakatupunga he ngaahi ngauee kakaa ‘o e tekinolosia faka-Komipiuta. ‘E tokoni nai e fekumi faka-ako ni ke ‘ilo ha founga ke tau teuteu mo lava ke mapule‘i e palopalema ‘o e ngaue kakaa ‘o e ngaluope?*

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

16. *Kataki fakamatala‘i ho‘o ‘uhinga fakatatau ki ho‘o fili ‘i ‘olunga*).

_____

_____

_____

_____

_____

17. *Kapau ‘oku ke tui ki he fakakaukau ‘o e‘**Tala ke i Kapa na’a ke tō ki Mala’**, kataki fakamatala angee ‘a e founga ho no nague‘aki e fakakaukau ni ke mapule‘i ‘aki e ngaaahi faihia faka-Komipiuta ‘i Tonga ke fakasi‘isi‘i ha ngaahi palopalema? (Fakatataa, kapau ‘e fakahoko ha ngaahi polokalama ako ke ‘ilo ‘e he kakai etc..).*

_____

_____

_____

_____

_____

18. *Kapau ‘oku ke ‘IKAI ke ke tui ki he fakakaukau ‘o e ‘**Tala ke i Kapa na’a ke tō ki Mala’**, kataki fakamatala angee ki he ‘uhinga ‘oku ‘IKAI k eke tui ai ki he fakakaukau ni?*

_____

_____

_____

_____

_____

B. Kavei Koula ‘a e Tonga

Ko e ngaahi Kavei Koula ‘a e Tonga; (***faka’apa’apa, tauhi-vā, mamahi’ime’a, lototō mo e ‘ofa***) ‘a e ngaahi tefito’i makatu’unga tefito ‘o e ‘ulungaanga faka-Tonga. ‘Oku polepole ‘a e Tonga he ngaahi tefito’i makatu’unga koula ko ‘eni, pe a ‘oku nau loto ke tauhi, ngaue’aki pe a paasi ki he ngaahi to’utangata ki laloo. ‘I ha tu’unga ku o ke ‘ilo ki ha taha ho famili pe maheni ofi ‘oku ne fakahoko ha ngauehala ‘o maumaui’i e laoo ‘o e fonua ‘o hangee ngaahi faihia ‘o e Ngaluope mo ha ngaahi hia kehekehe pe. Ko e haa ho’o me’a ‘e fakahoko?

19. *Te ke lipooti ki he kau polisi/ pe taki-Potungaue/ ’ofisa-kolo pe kau ma’u mafai ’e ne faihala*?

A. ‘Io B. ‘Ikai C. ‘Ikai fakapapaui’i

20. *Kapau ko ho’o tali ki he fehu’i ’i ’olunga ’oku ’IKAI, ko e ha leva e ’uhinga lelei ’oku ’ikai te ke loto ai ke lipooti te ke loto ke tala kau polisi/ pe taki-Potungaue/ ’ofisa-kolo mo e kau ma’u-mafai?*
(Kataki ‘o fili ho’o tali he ‘u puha ‘i lalo pea ‘oku lava pe ke fili ‘o lahiange he tali ‘e taha (1)).

A. ‘Oku ou *faka’apa’apa’i* ‘aupito e tokotaha ni pea ‘oku ou loto pe ke u tauhi ‘e ku *faka’apa’apa* ki he tokotaha ni ‘o ‘ikai te u lipooti ia ki he kau ma’u mafai

B. ‘Oku ou *’ofeina* ‘aupito e tokotaha ni pea ‘oku ou loto pe ke u tauhi ‘e ku *’ofa* ki he tokotaha ni ‘o ‘ikai te u loto ke too ki ha faingata’a (fakatataa; ha’ane ‘alu ngaue popula he ‘oku ‘i ai ho no fatongia ki ho no famili).

C. Koe’uhi ‘oku ou loto pe ke *tauhi hoku vaa* mo e tokotaha ni, ko ia ‘oku ou loto pe ke tauhi e vaa ke tu’uloa pe a ‘ikai fiema’u ia ke lipooti ki he kau ma’u mafai.

D. ‘I he’eku loto-fakato-ki-lalo mo *lototō* ki he tokotaha faihia, ko e makatu’unga lelei ia ke ‘oua te u kaunoa mo fiekau ke lipooti ki he kau ma’u mafai a e ngaue hala ni.

E. Kuo tuku mai ‘a e falala ‘a e kakai mo e komiunitii kiate au koe’uhi ko ‘e ku mamahi’i-ho-ku-ngaahi-fatongia (*mamahi’ime’a*). Kapau te u lea ‘o tala, ‘e mole e falalala meite au koe’uhi ko ‘eku lea he ngaahime’a ‘oku ‘ikai totonu ke u lea ai.

F. Takitaha nofo ‘o tokanga’i kita ‘oua ‘e kaunoa he ngaahi pisinisi ‘a e kakai ke he he ‘oku ‘ikai ha’ate ‘ilo na’a vilo mai e palopalema tatau kiate kita. ‘Oku ‘i ai pe kakai totonu ke nau fakahoko e ngaahi fekumi ki he ngaahi faihia ‘o e Ngaluope.

G. Ngaahi ‘uhinga makehe, kataki ‘o fakahaa ho’o tali he kolomu ‘i lalo

_____

_____

_____

_____

_____

21. *Fefee kapau ko e tokotaha ko ia (faihia) ʻoku ʻikai ko e famili pe ko ho kaumeʻa mamae? Kataki fakamatalaʻi angee hoʻo meʻa ʻe fakahoko?*

_____

_____

_____

_____

_____

22. *Fefee kapau ko ha tokotaha ʻoku taki ʻi he koloo, houʻeiki, tokotaha takilotu, tokotaha maʻolunga he Puleʻanga, pe ko ha kakai taki ʻi he fonua. Ko e haa hoʻo meʻa ʻe fai? Te ke ke loto ai pe ke lipooti ai pe kinautolu ki he kau maʻu mafai pe kau Polisi?)*

A. ‘Io B. ‘Ikai C. ‘Ikai fakapapaui’i

23. *Kataki fakamatalaʻi hoʻo ʻuhinga fakatatau ki hoʻo fili mo hoʻo tali ki he fehuʻi ʻi ʻolunga*

_____

_____

_____

_____

_____

C. Tahi Kulokula (Sea of Red)

Ko e fakakaukau ‘o e **Tahi Kulokula** (**Sea of Red**) ‘oku ‘i ai pe ho no ngaahi ‘uhinga kimu’a, ka ne toki mahino kimui mai he taimi ne teunga kulokula ai ‘a e kakai Tonga. ‘Oku ‘ikai fu’u nofo taha pe ki

he naaghi kavei koula ‘a e Tonga ka ‘oku ne fakahaa ‘a e uouongataha mo e laumalie-taha ‘a e kakai ‘o Tonga. ‘I he ngaahi ta’u mai ki mui ni mai, ko e kakai ne nau teunga kulokula ke fahamahino ‘e nau faka’apa’apa kiate kinautolu fanau va’inga konga-Tonga me i muli (va’inga liiki mo e ‘akapulu) ne nau loto ke fakafofonga’i ‘a Tonga, ko e fonua honau tukufakaholo. Ko e kau mai ‘a e fanau va’inga ‘oku ‘ikai ngata pe he’eneu talangofua ki he’enau matu’a ka ‘oku na u fakahaa ‘e nau *faka‘apa‘apa, lototō, tauhi-vā, ‘ofa* mo e *mamahi‘ime‘a*. Kapau ‘e ‘uuni fakataha e fakakaukau ‘o e Tahi Kulokula mo e ngaahi kavei koula ‘a e Tonga, ‘e malava ko e maka fakava’e fefeka ke taui’i ‘aki ‘a e palopalema ho no fakaehaua e kainanga e fonua he ngaahi ngaue ‘oku ‘ikai totonu ‘o ka u ai e ka u fakakina ‘o e Ngaluope. Ko e Tahi Kulokula ‘oku ne fakafofonga’i e lototaha pe ‘ikai to e fakakouna, ka ko e ngaue fakataha he ko e kakai pe ‘e taha mo e Pule’anga pe ‘e taha ke taui’i e fa’ahinga kakai ngaue faka-tevolo ni. Ko e ‘atakai mo ‘etimosifia ‘o e Tahi kulokula ‘oku ne ‘omai ‘a e uouongataha, laumalie-taha, ngaue fakataha, loto mafana, mo e ‘ofa ‘a e Tonga. Kapau ‘e ‘omai e ngaahi ‘uuni ‘elemeniti ni mo e ngaahi loto ko ia ‘o ngaue’aki ‘e hoko leva ia ko e ngaahi makatu’unga lelei ke tokoni ki ho no ke taui’i ’aki e ngaahi ngaue ‘oku ‘ikai totonu he ngaluope ‘i Tonga mo ha to e ngaue ‘ikai totonu pe.

24. *Ko e Tahi-Kulokula ‘oku fakafehoanaki ki he lototaha pe ‘ikai to e fakapu‘ia ke ngauefakataha. ‘Oku ke tui ko e fakakaukau ‘o e Tahi-Kulokula ‘e malava ke ne tokoni ki ho no mapule‘i e tupu ‘a e ngauee kakaa ‘o e ngaluope ‘i Tonga?*

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

25. *Kataki fakamatala‘i ho‘o ‘uhinga fakatatau ki ho‘o fili ‘i ‘olunga*

_____

_____

_____

_____

_____

26. *Kapau ‘oku ke tui ki he fakakaukau ‘o e Tahi Kulokula (Sea of Red), kataki fakamatala angee ‘a e founga ho no nague‘aki e fakakaukau ni ke mapule‘i ‘aki e ngaaahi faihia faka-Komipiuta ‘i Tonga?*

_____

_____

_____

_____

D. Mate ma'a Tonga (Die for Tonga)

Ko e 'Mate ma'a Tonga' ko e kaveinga motu'a pe ia ne ngaue fuoloa mai 'aki 'i Tonga ka ne to e manakoa ange ho no ngaue'aki he'e timi liiki fakafonua 'a Tonga 'o fakahingoa ko e Mate Ma'a Tonga. Ko e kaveinga tatau pe ia he 'Tahi Kulokula' ne ngaue'aki 'e he fanauva'inga ke nau li'aki 'a e ngaahi monu'ia faka-pa'anga he'enau va'inga he ngaahi timi muli ka nau foki 'o fakafofonga'i 'a Tonga.

27. *Ko e fakakaukau 'o e Mate ma'a Tonga 'oku fakafehoanaki ki he 'ofa fonua pe 'ofa ki Tonga. 'Oku ke tui ko e fakakaukau 'o e 'ofa fonua pe a mo e kaveinga 'o e* ***Mate ma'a Tonga (Die for Tonga)****, 'e malava ke ne tokoni ki ho no mapule'i e tupu 'a e ngaues kakaa 'o e ngaluope 'i Tonga?*

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

28. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga*

_____

_____

_____

_____

_____

29. *Kapau 'oku ke tui ki he fakakaukau 'o e* ***Mate ma'a Tonga (Die for Tonga)****, kataki fakamatala angee 'a e founga ho no nague'aki e fakakaukau ni ke mapule'i 'aki e ngaaahi faihia faka-Komipiuta 'i Tonga?*

_____

_____

_____

_____

_____

30. *Kapau 'oku 'IKAI ke ke tui ki he fakakaukau 'o e* ***Mate ma'a Tonga (Die for Tonga)****, kataki fakamatala angee 'a e'uhinga 'oku 'ikai k eke tui ai ki he fakakaukau ni?*

_____

_____

E. Mate pe Tonga he ngaue ‘a e Tonga (Tongan-kills-Tongan)

Ko e fakakaukau ‘o e ‘***Mate pe Tonga he ngaue ‘a e Tonga’*** (**Tongan-kills-Tongan**) ‘oku ‘ikai ko e ‘ohofi ke tamate’i. Ko e palani ke takihala’i pe kakai’i ha taha pe kakai ‘i he nofo ‘a e Tonga. ‘I he fakakaukau ni, kapau kuo ‘osi ma’u ha taha ‘i he ngaahi ngaue kakaa ‘o e ngaluope, ‘e malava he’e tokotaha ko ia ke ne to e fa’u ‘e ia ha palani ke to e ma’u atu mo ha kakai kehe koe’uhi ke nau tatau kotoa pe. ‘I he taimi ‘e lava ai e palani ‘a e tokotaha pe kakai kuo ‘uluaki ma’u kinautolu ki mu’a ke takihala’i e kakai lotoma’a ke nau kaungaa ‘efihia fakataha, kuo a’u mo mo’oni leva e fakakaukau ‘o e ‘***Mate pe Tonga he ngaue ‘a e Tonga’***. Ko e fehu’i, ‘e malava nai ke hoko ‘a e fakakaukau ni ‘***Mate pe Tonga he ngaue ‘a e Tonga’*** ‘e he kakai na ‘e ‘uluaki ma’u kinautolu ki mu’a ke ne takihala’i e kakai lotoma’a mo te’eki ke nau ‘efihia ke nau ‘efihai tatau pe he fa’ahinga to’onga ngaue kakaa ni?

31. ‘*Oke ke ma’u ki ha taha na’a ne ‘osi fakahoko ha fa’ahinga ngaue pehee ni kiate ko e pe kakai ke he, ke ‘efihia tatau pe he ngaahi ngaue ni?*

A. ‘Io B. ‘Ikai C. ‘Ikai fakapapaui’i

32. *Kapau ko ho’o tali ‘Io, kataki fakamatala ki he founga na’e ne fakahoko ‘aki e ngaue ni?*

_____

_____

_____

_____

_____

33. *Na’a ke ‘osi fakahoko ha fa’ahinga ngaue pehee ni ki ha kakai ke he?*)

A. ‘Io B. ‘Ikai C. ‘Ikai fakapapaui’i

34. *Kapau ko ho’o tali ‘Io, ko e ha e ‘uhinga na’a ke fakahoko ai e ngaue ni ki he kakai*?

_____

_____

_____

_____

_____

35. *Kataki fakamatala ki he founga na’a ke fakahoko ai e ngaue ni*?

_____

_____

_____

_____

_____

36. *'Oku ke ongo'i fakatomala ki ho'o ngaue na'e fakahoko ki he kakai*?

A. Io B. 'Ikai C. 'Ikai fakapapaui'i

37. Kataki fakamatala ki he 'uhinga ho'o tali 'i 'olunga?

_____

_____

_____

_____

_____

38. *Kapau ne te'eki ke hoko ha fa'ahinga ngaue pe he ni, 'oku ke tui 'e malava ha'a taha kuo 'osi ma'u pe 'efihia kimu'a he fa'ahinga ngaue panngo ni ke ne fakahoko ha me'a tatau ki he kakai 'o Tonga ke nau 'efihia tatau pe*?

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

39. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga*

_____

_____

_____

_____

_____

F. Fakapulipuli (Privacy)

Angamaheni'aki, ko e kakai Tonga 'oku nau fakalonglongo pe a 'ikai lava ke nau vahevahe honau ngaahi palopalema ke to e 'ilo'i ha'a taha pe kakai ke he. "Ikai ke nau vahevahe ke 'ilo na'a nau 'efihia ha palopalema koe'uhi ko e luma ta'engata kiate kinautolu pea toe holoki honau tu'unga langilangi

honau famílii. Kapau kuo ma'u ha'a taha he ngaahi ngaue kakaa 'o e Ngaluope 'e malava ke hoko ia ko e luma fakafamili kapau 'e mafola e talanoa ko ia ki he maheni, famili mo e kolo foki. Ko e mofele vave 'o e talanoa 'i Tonga 'oku vave 'aupito koe'uhi 'oku meimei fe'ilongaki e tokotaha kotoa pea kanoni'aki ko e komiunitii si'isi'i.

40. *'Oku ke fakakaukau kapau 'oku 'i ai ha palopalema 'oku totonu nai ke vahevahe honau ngaahi palopalemaa ke 'ilo'i, fakatataa, kakai ne 'osi ma'u he'e ngauee kakaa 'o e ngaluope ke vahevahe na'a 'i ai ha fa'hinga tokoni kiate kinautolu ke solova e palopalema 'o 'oua 'e kukuta pe fakapulipuli'i.*

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

41. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga*).

_____

_____

_____

_____

_____

42. *Fefee kapau na'a ke loto ke fakahaa ho'o palopalema ke 'ilo ki ai ha taha, kataki fakamatala ange ki he 'uhinga ho'o tali (pe tali 'oku fai)?*

_____

_____

_____

_____

_____

43. *Kapau na'e 'ikai te ke loto malohi/pe 'ikai loto ke fakahaa ho'o palopalema ke 'ilo ki ai ha taha, kataki fakamatala ange ki he 'uhinga ho'o tali (pe tali 'oku fai)?*

_____

_____

_____

44. *Ko e fakalongolongo ʻo ʻikai fakahaa e palopalema (fakatataa, kapau kuo maʻu ʻe he kaufakakina ʻo e ngaluope) ʻe ʻikai malava ke ʻi ai ha makatuʻunga malohi ke fakahokoʻaki ha fekumi ke solova e palopalema ni. Ko e haa ha faleʻi pe fokotuʻu fakakaukau ke lava ʻo vahevahe e palopalema ke ʻilo ki ai e kainga-ofi pe kau maʻumafai ke fekumi ha solovaʻanga ki he palopalema?*

G. Tui Faka-Kalisitiane pe Tui Faka-Lotu (Religious belief)

Ko e lotuu mo e tui Faka-Kalisitiane ʻa e ngaahi huʼituʼa lalahi ʻo e moʼui ʻa e Tonga. Ko e kau Faifekau mo e kau Setuata ʻa e fakakaukau ko kinautolu ʻa e fakafofonga ʻo e ʻOtua pe Kakai ʻa e ʻOtua. Ko e ngaahi fekau me i he tohitapu ʻoku tufaki mai ʻe he Kakai ʻa e ʻOtua ʻoku fakamuʻomuʻa, fakalanglangiʻi pea muimui ki ai ʻa e kakai ko e fakahaa ʻo e tui ki he ʻOtua ʻoku moʻui. Ko e ʻikai muimui ki he ngaahi fekau ʻoku akonekina mai ʻe he Kakai ʻa e ʻOtua ko e ngaue ʻoku ʻikai faka-Kalisitiane pe a ʻoku fakafepaki ia mo e Folofola ʻa e ʻOtua. Ko e ngaahi akonekina ʻoku ʻomai ʻe he Kakai ʻa e ʻOtua ke nofo anganotonu mo e ʻoua ʻe fakahoko e ngaahi ngaue faka-Tevolo, ka u ai ʻa e ngaahi ngaue kakaa ʻi he Ngaluope. Fakatataa, ko e feinga ke kaungahia pe ʻefihia ʻa e kakai faitotonu ke nau too ki ha faingataʻa ko e angahala ia ʻoku fakatau ki he malaʻia. Ko e totongi ʻo e angahala ko e mate.

45. *Kapau ʻe ʻoatu ha fekau me i he kau taki-Lotuu ki he kakai ke na u angatonu mo fakamamaʻo me i he ngaahi palopalema faihia faka-Komipiuta, ʻoku ke tui ʻe tali ʻe he kakai Tonga ʻe faleʻi*?

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

46. *Kataki fakamatalaʻi hoʻo ʻuhinga fakatatau ki hoʻo fili ʻi ʻoluŋga*).

47. *'Oku ke fakakaukau ko e ngaue ko 'eni ki ho no kakai'i e kakai (Tonga mo e 'ikai Tonga) 'e he kau fakakina e Ngaluope, ko e angahala pe a 'oku fepaki mo e tui faka-Kalisitiane*?

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

48. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga*).

_____

_____

_____

_____

_____

49. *'Oku ke tui 'e tokoni 'e tau tui faka-lotu ki he 'Otuaa ke tokoni ki ho no fakasui'isi'i e ngaahi palopalema 'o e ngaue kakaa he ngaluope tanaki atu ki ai m o e ngaahi akonekina 'oku 'omai me i he kau Faifekau mo e kau Setuata?*

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

50. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga*

_____

_____

_____

_____

_____

51. *Kapau 'oku ke 'ilo ko e tui faka-Lotu ki he 'Otua 'oku mo'ui 'e tokoni ke fakasi'isi'i e palopalema ki he ngaushala'aki 'o e ngaluope, kataki fakamatala pe 'e anga fefee 'e ne tokoni*?

_____

_____

_____

_____

_____

H. Fakatu'utu'unga e nofo (Hierarchal Rank)

'I he fa'unga fakatu'utu'unga 'o e nofo faka-Tonga, ko e Tu'i 'oku mafai ma'olunga taha, hoko ki he kau nopele, mo e kakai 'i he taupotutaha ki lalo. 'Oku makehe 'aupito e anga e mo'ui 'a e Tonga he fa'unga fakatu'utu'unga (Hierarchal Rank) 'o e nofo faka-Tonga kamata me i he taupotu ki 'olunga (Tu'i) 'o movete ki he ngaahi fa'unga 'i lalo (kakai). Kakai 'a e taupotu taha ki lalo 'i he fa'unga e nofo pea kuopau ke nau faka'apa'apa ki he ngaahi fekau he ko kinautolu (Tu'i, hou'eiki 'oku ma'olunga ange) 'oku nau ma'u 'a e mafai lahi.

52. *'Oku ke fakakaukau pe fakatokanga'i e kakai Tonga mo e hakotupu 'oku nau ke i tauhi mai e fa'unga 'o e nofo faka-Tonga (Tu'i, Ho'u'eiki, Kakai) he ngaahi 'aho ni*?

A. Io B. 'Ikai C. 'Ikai fakapapaui'i

53. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga.*

_____

_____

_____

_____

_____

54. *Kapau 'e 'i ai ha fekau pe tu'utu'uni me i 'olunga (kau nopele, matapule pe 'ulumotu'a) ki he kakai ko e kainga e fonua ke nau tokanga ki he ngahi hia faka-komipiuta. 'Oku ke tui 'e tali lelei 'e he kakai kainanga e fonua e fekau?*

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

55. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga*

_____

_____

_____

_____

_____

56. *Oku ke tui 'oku ke i mahu'inga ki he Tongaa ke na u tauhi e ngaahi tukufakaholo 'o e nofo faka-Tonga ko e tauhi-va 'a e kakai kainanga e fonua ki he kakai 'oku nau 'i 'olunga*?

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

57. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga*

I. Lea Faka-Tonga

'Oku hoko ho no ngaue'aki 'o e Tekinolosia faka-Komipiuta ko e tokoni lahi ki he kakai Tonga, hangee ko e talanoa hangatonu ki he ngaahi famili ki muli, sio pe me i he ngaahi lotofale ki he ngaahi me'a 'oku hoko 'i mamani, lava pe 'o fakahoko e fe'aveaki pa'anga 'o 'ikai to e fiema'u ke 'alu ki he Pangike ke talafi e seniti ki Tonga/muli etc. Kaikehe 'i he tafa'aki 'e taha, 'oku hoko ha ngaahi maumau ki he fa'unga e lea faka-Tonga, hangē ko e tohi nounou 'o 'ikai kakato (e.g. tangata - tohinounou ko e tgt, sio - tohinounou ko e co, telefoni – tohinounou ko e pH, etc), tuifio e lea-Tonga mo e lea faka-Palangi, 'ikai ngaue'aki e faka'ilonga toloi, fakamamafa pau̇, komaa, etc.

58. *Oku ke tui 'oku maumau lahi e fa'unga 'o e lea faka- Tongaa 'o hangē ko ia 'oku fakamatala 'i 'olunga*?

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

59. *Fēfē leva 'a e ngaahi lea 'ikai-fe'unga 'oku ngaue'aki 'e hotau kakai ki he'enau ngaahi tohi (post) 'oku tukumai he Ngaluope. 'Oku ke tui 'oku ne maumaui'i 'a e faka'apa'apa, lototō, tauhi-vā, mamahi'ime'a mo e 'ofa?*

Strongly Disagree	**Disagree**	**Unsure**	**Agree**	**Strongly Agree**

60. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga*

61. *Kuo ʻau ʻeni ki ha tuʻunga kuo ngaueʻaki e he kakai e fonua ke kakapa hake ʻe nau lea ki he Tuʻi ʻo Tonga (hufanga he fakatapu) mo e ka u Nopele, ka naʻe pelepelengesi ʻi he taimi kimuʻa. Kuo mole leva e faʻunga e nofo ʻa e Tonga ʻi he ngaue ʻa e Tekinolosia. ʻOku ke tui ʻki he fakakaukau ko ia?*

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

62. *Kataki fakamatalaʻi hoʻo ʻuhinga fakatatau ki hoʻo fili ʻi ʻolunga*

_____

_____

_____

_____

_____

63. *Ko e haʻa hoʻo faʻahinga ongoʻi ʻiate ko e ki he ngaahi meʻa ʻoku hoko tonu ʻi ho no ngaueʻaki ʻe he kakai ʻa e Tekinolosia ʻo e Ngaluope ke nau kakapa ha ke ʻeni ʻo lea ki he Tuʻi ʻo Tonga (hufanga he fakatapu) mo e kau Nopele ʻo taku ko e totonu ke na u lea tauʻataina. Kataki ʻo fakamatalaʻi e ongo ʻiate ko e (e.g. fiefia, mamahi, pe ʻoku ʻikai te ke tokanga ko e ki ai etc.)*

_____

_____

_____

_____

_____

64. *Ko e haʻa hoʻo faʻahinga ongoʻi ʻiate ko e ki he ngaahi meʻa ʻoku hoko tonu ʻi ho no ngaueʻaki ʻe he kakai ʻo ʻikai tohi totonu ʻa e lea-Tonga ke tauhi ke maʻumaʻuluta mo totonu, he ʻoku maumau ai e faʻunga ʻe tau lea-Tonga ʻoku tau feinga ke tauhi ke tukufakaholo mo tolonga. Kataki ʻo fakamatalaʻi e ongo ʻiate ko e pe (e.g. fiefia, mamahi, pe ʻoku ʻikai t eke tokanga ko e ki ai etc.)*

_____

_____

_____

_____

65. *Ko e ha leva ha'o fale'i pe fakakaukau ki he palopalema ni mo ha founga ke ke i tauhi e molumalu e nofo 'a e kakai ke nau ke i tauhi pe ke ke i tu'uloa pe 'a e Tu'i 'o e 'Otu Tonga mo ho no kau Nopele pea faka'apa'apa'i pe 'e he kakai 'o Tonga ke tolonga mo tu'uloa. Kataki fakamatala'i ho'o 'uhinga.*

_____

_____

_____

_____

_____

J. Ngaahi fēveitapui

Ko e faka'apa'apa mo e tapu 'i he nofo 'a e tuonga'ane mo e tuofefine 'oku taha pe a makehe ai 'a Tonga. Fakatataa, ko e tuonga'ane 'oku 'ikai ngofua ke huu ki he lokimohe ho no tuofefeine, 'ikai ngofua ke talanoa noa'ia ha ngaahi lea 'ikai taau, tapui ke ofi ki he ha'ofanga inukava 'oku ***tōu'a*** ai ho no tuofefine mo ha ngaahi fakataha'anga faka-tamaiki etc. Ko e fēveitapui ko ia 'oku 'i ai leva e faka-ngangata he vaha'a 'o e tuonga'ane mo e tuofefine ke na talanoa ki ha ngaahi palopalema faka-ē-kinau (personal) pe. 'Ikai ngata ai ka ko e fakafe'atungia ki ho no vahevahe ha ngaahi fakapulipuli ko e 'uhi ko e fakangatangata 'o e lea (talanoa noa'ia ha ngaahi lea 'ikai taau) pe a 'ikai lava ke tau'ataina ke vahevahe he'e tokotaha ko ē ki he tokotaha ko ē kapau 'oku faingata'a'ia ha tokotaha.

66. *'Oku ke tui 'oku hoko 'a e feveitapui'aki ke 'ikai tau'ataina ai 'a e tuonga'ane mo e tuofefine ke na vahevahe tau'ataina ha palopalema 'oku hoko 'iate kinaua ka 'oku 'ikai ke lava vahevahe ko e feveitapui'aki?*

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

67. *Kataki fakamatala'i ho'o 'uhinga fakatatau ki ho'o fili 'i 'olunga*

_____

_____

68. *Ko e ha leva ha fokotu'u fakakaukau kihe kaveinga ni mo ha ngaahi me'a ke fakalelei kapau he 'oku tau polepole he feveitapaui 'a e tuonga'ane mo e tuofefine pe a 'oku 'ikai ha fonua 'i mamani 'oku nau fakahoko ha founga pe hee ni, ngata pe 'a Tonga 'oku nau fakahoko e feveitapui'aki. Ko e ha leva ha'o tokoni ki ha ngaahi me'a ke fakalelei'i kapau 'oku 'i ai ha me'a ke tanaki mai?*

_____

_____

_____

_____

_____

_____

69. *'I he fakakaukau faka-lukufua, 'oku 'i ai nai ha'o fokotu'u ki ha founga 'e tokoni ki hotau kainga Tonga ke ta'ota'ofi'aki e palopalema fekau'aki mo e ngaue kakaa he Ngaluope?*

_____

_____