YANGON UNIVERSITY OF ECONOMICS
MASTER OF DEVELOPMENT STUDIES PROGRAMME

A STUDY ON CYBERCRIMES AWARENESS OF INTERNET USERS IN YANGON

YADANAR SEIN
EMDevS – 55 (16th BATCH)

DECEMBER, 2020

YANGON UNIVERSITY OF ECONOMICS

MASTER OF DEVELOPMENT STUDIES PROGRAMME

A STUDY ON CYBERCRIMES AWARENESS OF INTERNET USERS IN YANGON

A Thesis submitted in partial fulfillment of the requirements for the Master of Development Studies (MDevS) Degree

Supervised by

Dr. Cho Cho Thein
Professor (Head of Department)
Department of Economics
Yangon University of Economics

Submitted by

Yadanar Sein
Roll No – 55
EMDevS 16th Batch
(2018 - 2020)

December, 2020

YANGON UNIVERSITY OF ECONOMICS
DEPARTMENT OF ECONOMICS
MASTER OF DEVELOPMENT STUDIES

This is to certify that this thesis entitled **"A STUDY ON CYBERCRIMES AWARENESS OF INTERNET USERS IN YANGON"** submitted as a partial fulfillment of the requirement for the Degree of Master of Development Studies has been accepted by the Board of Examiners.

BOARD OF EXAMINERS

Dr. Tin Win
(Chairman)
Rector
Yangon University of Economics

Dr. Ni Lar Myint Htoo
(Examiner)
Pro-Rector
Yangon University of Economics

Dr. Kyaw Min Htun
(Examiner)
Pro-Rector (Retired)
Yangon University of Economics

Dr. Khin Thida Nyein
(Examiner)
Pro-Rector
Yangon University of Economics

Dr. Tha Pye Nyo
(Examiner)
Professor
Department of Economics
Yangon University of Economics

Dr. Cho Cho Thein
(Supervisor)
Professor and Head
Department of Economics
Yangon University of Economics

ABSTRACT

Myanmar becomes one of the countries threatened by cybercrimes. This study intends to examine the level of cybercrime awareness of Internet users in Yangon and to identify the type of cybercrime used to happen in Yangon. The descriptive method was used. The primary data are collected by snowball sampling method. The survey was conducted with structured questionnaires to 1071 respondents. The study found that cyber harassment among the cybercrimes happening in Myanmar was the highest case. The second highest case is cyberbullying and fraud is the third. International standard Cyber Law was needed to enact and law enforcement was weak. The respondents were weak in cybercrimes awareness levels and regulations related to cybercrimes. The most known law by respondents was Telecommunication law (66D). The Respondents' most experiences were Fraud, Cyberbullying and Cyber harassment cases. Female respondents were prone to cybercrimes than male respondents. The fraud case was used to happen in Yangon internet users. To increase cybercrimes awareness levels, Government should provide digital skills curricula regarding the cyber advantages and disadvantages in the school and cybercrimes awareness training or campaigns for the community.

ACKNOWLEDGEMENTS

Firstly, I would like to describe my grateful appreciation to Professor Dr. Tin Win, Rector of Yangon University of Economics, Professor Dr. Ni Lar Myint Htoo, Pro-Rector of Yangon University of Economics and Programme Professor Dr. Cho Cho Thein (Head of Department), as well as my supervisor who supported me with heart and soul throughout the whole process and gave guidance so that I could accomplish this paper. Not only did she provide me with guidance and further reading, but also did she spare her time to read my paper despite the fact that she was fully occupied with her time. Moreover, I am thankful for her patience, valuable advice, and supervision while working on the paper. Without her guidance and support, I would not be able to make this happen.

Secondly, I would like to thank Professor Pro-Rector (Retd.) U Kyaw Min Htun who gave me guidance and supported me during my trying period of Thesis writing. Thirdly, I would like to express my deep gratitude to Professor Dr. Khin Thida Nyein, Pro-Rector of Yangon University of Economics and Professor Dr. Tha Pye Nyo who strongly guided and supported me during the time I had been writing my Thesis until the time I completed. Finally, I would like to thank all of my EMDevS 16th Batch classmates especially my beloved Group (7), my best friends, and my colleagues, for supported and encouraged me during the time I met hardships, problems.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREBIATIONS

AMPS	Advanced Mobile Phone System
ATM	An automated teller machine
ADSL	Asymmetric digital subscriber line
CDMA	Code Division Multiple Access
CATV	Community Access Television
CSIS	Strategic and International Studies
CCIFRANCE	French Myanmar Chambers Of Commerce & Industry
DECT	Digital Enhanced Cordless Telecommunications
EIGE	European Institute for Gender Equality
FTTP	Fiber to the Premises
FBI	Federal Bureau of Investigation
GSM	The Global System for Mobile Communications
IXP	Internet exchange point
IT	Information Technology
ICT	Information Communication Technology
IP	The Internet Protocol
INTERPOL	The International Criminal Police Organization
MSN	Microsoft Network Messenger
MCF	Myanmar Computer Federation
MCPA	Myanmar Computer Professionals Association
MCIA	Myanmar Computer Industry Association
MCF	Myanmar Computer Federation
MCEA	Myanmar Construction Entrepreneurs Association
MDGs	Millennium Development Goals
McWill	Multi-carrier Wireless Information Local Loop
mmCERT	Myanmar Computer Emergency Response Team
NASA	The National Aeronautics and Space Administration
OS	Operation System
PCO	Public Call Offices
PwC	PricewaterhouseCoopers
SCPC	Single channel per carrier
SEA-ME-WE 3	South-East Asia - Middle East - Western Europe 3

SIM	A subscriber identity module
SME	Small and medium-sized enterprises
UNFPA	The United Nations Population Fund
WSIS	The World Summit on the Information Society
VAST	Viewer Access Satellite Television service
VoIP	Voice Over Internet Protocol
VTC	Video Teleconferencing Platforms
WCDMA	Wideband Code Division Multiple Access

CHAPTER I

INTRODUCTION

1.1 Rationale of the Study

In the age of globalization, the development of the ICT sector contributes to the world economy by increasing productivity, promoting economic development, and reducing inequality and poverty. According to United Nation and World Bank argued that the ICT sector is the key driver of Sustainable Development. ICT has positive effects on economic development, productivity, and employment. The internet helps people in providing information and storing valuable information data related to personal, business, government data. The internet has become so crucial and became an essential part of people's lives. Nevertheless, due to the increase of modern technology, it has become very difficult to keep safe people's private information and data. The data are becoming easily accessible to people around the globe. This has becomes leads to an increase in crime such as anyone can access one's personal data without the high technology and knowledge. Therefore, cybercrime becomes inevitable in the social and economic environment of every country.

Today, the modern Internet has evolved into an essential requirement for almost everything by several operating systems development (OS), such as Android OS, Windows OS, Mac OS, IOS, etc.,. It brings the banking sectors developed for daily banking transitions. People can use modern smart device to check bank accounts balances, making money transitions, make internet calls, learning online course, shop online, etc. These facilities play a huge role in daily needs and the banking world. The Internet became a relief for the modern age but also causes a burden on people. It also transformed a new kind of crime, called cybercrime. Common internet users are unaware of cybercrimes. People don't know the correct preventing methods to keep such assaults from taking place. Many people have been suffered from individual cybercrimes across the globe. To commit cybercrimes, only computers or mobile & smart devices and internet access are required for the criminal. Cybercrimes involved

hacking, identity theft, credit/debit card fraud, cyberbullying, etc. Cybercrimes can happen to anyone who using internet platform services.

In line with the development of E-commerce, E-business, E-banking, on other hand, cybercrimes evolved across the countries especially in developed countries rather than developing countries. Because it depends on the development situation of the ICT system. Based on the data from the VARONIS website described that Hacker attacks every 39 seconds, on average, 2244 times per day, and 4.1 million data records were destroyed during the first half of 2019(Sobers, 2020).

In this context, Myanmar has developed in internet services and increasing internet users, the data from the Datareportal (2020), Myanmar has 22 million Internet users (41 percent of the total population). Especially this population was increased after reformed in telecommunication sectors and private sectors investment. With inexpensive SIM cards and a stable 2G, 3G, and 4G network infrastructure, Internet connectivity has grown in Myanmar. The Data from Ccifrance Myanmar organization, Myanmar is in the midst of a large scale digitalization process, with an increasingly increasing telecommunications infrastructure and resulting in enhanced connectivity (Naon et al., 2018). This ICT development in Myanmar has a positive effect on all of the economic sectors especially huge development in Banking sectors, the effect of internet services development on the Myanmar banking sectors has the various requests from customers for widely banking services. Myanmar banking sectors extended their services to the online platforms. And also, with ICT sector development, Myanmar people have widely used various social media & internet platforms, Email, and online money transition. While the new-found connectivity and digitalization bring many improvements and opportunities with it, it also opens the doors to an entirely new threat of cybercrimes.

As reported by UNFPA (2015), Yangon 2014 census data, 60.9 % of the Yangon population were using Mobile phones and the internet. In the year 2020 in Yangon, there have main 26 internet services providers companies these internets services providers provided a verity of internet services such as Mobile Data internet, Wi-Fi broadband, Fiber internet, etc. The estimated population of internet users in Yangon is about 3.7 million and it has 70 percent of the total population (5.3million).

Yangon, is the capital city, biggest city, and most developed city of Myanmar. Pursuant to the most developed city, there was a great opportunity for education and the first touching of modern technology, etc. So, the people from Yangon can be

assumed that more modernize than other cities. Then the highest rate of internet users in Myanmar. In line with the development of internet services in Yangon, the cybercrimes rates are rising day by day. The awareness of cybercrime is very much needed in society. Because the Internet provides business communication with great advantages and the best way to communicate with clients & customers. So that this study highlights cybercrimes awareness levels and identifies the type of cybercrimes used to happen in Yangon.

1.2 Objectives of the Study

This study aims to examine the level of cybercrime awareness of Internet users in Yangon and to identify the type of cybercrimes used to happen in Yangon.

1.3 Method of Study

This study was applied the descriptive method with the quantitative approach by using the snowball sampling method in order to fulfill the objectives of this study. A survey was conducted with structured questionnaires for collecting the primary data via face to face interviewing as well as conducting online surveys. There were totally about 1071 respondents. They were internet users in Yangon and from many different layers. The secondary data was also collected from many sources, including literature, journals, and articles that related to the subject matters.

1.4 Scope and Limitations of the Study

This study is only focused on internet users living in Yangon to examine cybercrimes awareness levels and identify the cybercrimes case used to happen in Yangon internet users. As a limitation, this study cannot cover all internet users because the scope of the study is only focused on the Yangon area and the data were analyzed on the results of 1071 persons (out of 1200) due to the unknown population size of the internet users in Yangon Myanmar.

1.5 Organization of the Study

The study is organized into five chapters. Following this introduction, chapter one is rationale of the study, objective, scope and limitation, method, and organization of the study. Chapter two is the Literature review which consists of the concept, nature, and impact of cybercrime. Chapter three describes ICT and cybercrimes in Myanmar.

Chapter four is the survey analysis (case study) to examine the cybercrimes awareness and identify the cybercrimes case used to happen in Yangon internet users. The last chapter is the conclusion with the findings from the previous study and suggestions of the study.

CHAPTER II

LITERATURE REVIEW

2.1 Concept & Nature of Cybercrimes

According to Loader and Thomas (2000) as the earliest noted definition of Cybercrime, that was cybercrime is computer-mediated activities that are illegal or considered illicit by certain groups and may be carried out over global electronic networks. Casey (2004) also defined “Cybercrime as "any criminal act computers and networks, including crimes that do not depend heavily on computers". Hernandez (2018) states that Cybercrime refers to “any crime including a computer/mobile and a communications system could have been used to commit a criminal act or maybe the target" Cybercrime is an action carried out using computers and the internet.

According to Hernandez (2018) cybercrime began approximately in the 1960s, this includes theft of identities and critical information, breach of privacy and fraud, among others. Cybercrime has a primary financial effect, and cybercrime can involve several different forms of criminal activity driven by benefit, including malware attacks, email & online fraud, and intends to steal information from financial accounts, credit cards, or other payment cards as well.

Cybercriminals may target sensitive private information and business data for theft and resale (Rouse, 2020) .Cybercrime is multiplying like mushrooms and completely anonymous and cybercriminals were rationale. It is very difficult to track out who are cybercriminals and where they committed. Cyberspace is a new experience that is controlled by machines for information and communication between human beings around the globe. Therefore, crimes committed in cyberspace are to be dealt with as cybercrimes. Cybercrime is a threat to national and international socio-economic, global economic, political, and security systems. A new range of crimes known as cybercrime has arisen as a consequence of the improvement of technology.

Viswanathan (2001) has explained cybercrime’s nature is as follows: firstly, any criminal activity in which a computer is a tool or an object of a crime, in other words,

any crime, the means or the intent of which is to manipulate the operation of a computer. Second, any incident related to computer technology in which the victim suffered, or may have suffered, damage, and the perpetrator, knowingly, committed or may have done so again. Third, computer abuse is considered to be any illegal, unethical, or unauthorized conduct relating to the automated processing and transmission of data. According to Loader and Thomas (2000), the cybercrime has also been difficult for governments to control a flexible communications system designed to withstand attacks by rerouting messages. In order to identify criminal activity, anonymity also includes specialized computer skills.

The concept and general nature of cybercrimes can be used in two ways to attack the financial sector. The first one is direct and the other is indirect. Direct fraud includes credit and debit card fraud, and internet banking fraud. Indirect fraud includes scams, hacks, viruses, spam, and malware. Lottery scams, romantic scams, charities, pyramid schemes, and advance fraud are also frequently used. Some of the victims who received phone calls from the fake financial institute informed them that their accounts were frozen or inactive and cybercriminals asked for full information on account and password to maintain their account. Cybercrimes are made possible by the combination of computers or OS-based devices with telecommunications abilities (Luyali, 2011).

From the theoretical aspect, Cornish (2010) argued Rational choice theory[1] and cybercrimes (Cornish, 2010, as cited in Venkatasubbarao, 2013).The Rational Choice theory means that people are using rational calculations to think rationally and achieve results that are consistent by their own specific objectives (Ganti, 2020). In this rational choice theory, a single decision to commit a crime is based on the proportion of cost-benefit. "Rational" is the combination of personal costs and benefits in order to maximize personal gain. After weighing the prospective benefits against the possible risk, cybercriminals commit a crime. Via the internet, cybercrimes allow the attacker to do it from a relatively remote distance. The crime inflicts the same form of fear and intimidation as cybercriminals in the case of victims who are in a direct face-to-face situation. Rational choice theory is embraced by many people because it suggests that people behave in a rational manner. This indicates that many cybercriminals are very skilled and well educated and have the capacity to think rationally. They target the

[1] The rational choice theory originated during the late 18th century by Cesare Beccaria (Italian criminologist and economist) (Wright, 2009).

victims they believe would provide them with the greatest financial benefit and the least possibility of being caught. High-tech cybercriminals are very talented and difficult to catch because of the ability to cover their tracks and pass via proxy servers so that the cybercriminals, they are undetected, they commit massive fraudulent schemes and remain online undetected. The rational choice theory pointed out cybercrime has negative social and economic implications. This cybercrime has significant consequences on the technological, economic development of the nation including corruption, money laundering, leakage of military information, and terrorism (Venkatasubbarao, 2013).

2.2 Types and Behaviors of Cybercrimes

In today's high technology world, cybercrime is rapidly increasing. Criminals on the World Wide Web use information from Internet users to make their own gain. The cybercriminal can steal all of data through by internet. Even the government's confidential data were not secure by cybercrimes threat. Cybercrimes emerge in today's digital world in different forms and activities. Depending on cybercrimes activities and behavior, it can be categorized as cybercrimes "names and types";

Regarding the Cyber Harassment cases, Nuccitelli (2011) defined as the case of cyber harassment is the use of Information and Communication Technology (ICT) to harass, control, manipulate, or habitually disparage children, adults, companies, or groups without a direct or implicit threat of physical harm. Cyber harassment needs the use of Information Communication Technology and is verbal, sexual, social, and psychological harassment of the person, groups, or organizations.

According to Hernandez (2018) cybercrimes can be identified base on their activity as follows;

1. **Fraud** is described as a term of cybercrime that attempts to deceive an individual in order to obtain important information, money, or data.

2. **Hacking** includes the acquisition, in part or in full, of certain functions within a device, network, or website. It also aims at accessing crucial data and information, in violation of privacy. Most hackers target corporate and government data. There are many techniques and procedures for hacking.

3. **Identifying theft** is a particular type of fraud that steals personal data from cybercriminals, including passwords, bank account details, credit & debit cards detail, social security information, and other sensitive information.

4. **Scamming** is taking place in a number of ways. In cyberspace, scamming can be done by offering device repair, network troubleshooting, and IT support services, forcing users to pay cash for even non-existent cyber issues.

5. **Computer Viruses**, many criminals use viruses to access systems without authorization and to steal valuable data. Mostly, highly skilled programs send viruses, malware, and Trojans, to infect and destroy computers, networks, and systems. Viruses spread via the web and removable devices.

6. **Ransomware**, one of the most dangerous malware-based attacks is ransomware. It enters through computer network and, using public-key encryption, encrypts files, and information.

7. **DDoS or Distributed Denial of Service Attack**, among the hacking method it is one of most prominent hacking methods. Servers and networks that are properly running are temporarily or completely disrupted by DDoS.

8. **Botnets** are controlled by attackers from remotely called "bot herders" to make attack to computers by sending spam or malware. They typically target governments and corporations as botnets that directly attack the infrastructure of information technology.

9. **Spamming** uses digital communication protocols, most typically emails to send messages that contain viruses, false internet links, and other malicious behavior. Email spamming is really popular among everyone. It offers discounts, deals, and other enticing features for trick users.

10. **Phishing,** behave as a legitimate business or association. They use "email spoofing" to steal sensitive data such as credit card details numbers, social security numbers, passwords, etc.

11. **Social engineering** is one technique in which cybercriminals approach people directly through phone calls and emails. Basically, they are also going to behave like a legitimate business as well in order to get important information.

12. **Malvertising** is a term to define the technique of embedding malicious code to web-pages. Users will click on these ads which are actually fake. Once these advertisements are clicked, they will be redirected to fraudulent websites, or a file containing viruses and malware will be automatically downloaded.

13. **Cyberstalking** includes a person online who tracking anonymously. The stalker would virtually track the victim, regarding his or her activities. Most of the victims who suffered cyberstalking are women and children. Moreover, people committed to cyberstalking were men and pedophiles.

14. **Software Piracy**, the internet is loaded with channels and other services that illegally reproduce the original content, including songs, books, videos, records, and apps. This is a crime, as it translates into a violation of copyright.

15. **Child pornography** is a kind of sexual abuse of children. Child pornography refers to photos and videos of child sex abuse.

16. **Cyberbullying** is bullying that occurs on digital devices such as computers, mobile phones, and other ICT devices. Cyberbullying can happen via SMS, application, online platforms such as social media, online forums, and gaming these were people can accessible participate in sharing the content. The form of cyberbullying include sending negative content, sharing & posting, harmful, false content about some else.

2.3 Brief Overview of ICT Revolution and Cyberspace

Information Technology (IT) may be a collective term for the entire spectrum of technologies providing ways and means to accumulate, store, transmit, retrieve and process information. Information Technology isn't one technology but many, which have converged to serve the requirements of the knowledge revolution. Computing technology, Telecommunications, Audio, and Video technology, printing technology all are a part of it.

According to the historical records, the early information technology first developed in the USA was office machinery during the last quarter of the nineteenth century. The most popular equipment were typewriters, calculators, punched-card accounting machines, and filing systems. Introducing printing was the very first major advance in Information Technology. This made it possible for literacy and education to increase from 10% to over 80% by making vast amounts of reading material accessible within 50 years. In Europe, inventions such as electric telegraph, telephone systems, wireless or radio, television, broadcasting, computers have also led to the Reformation, which is another break-through for information technology (Pal, 2008).

The information revolution of these days is unquestionably prompted through the unprecedented advances in technology. Computers, Telecommunications, Micrographics, and Reprographics have emerged to provide a form to the acquainted segment acknowledged as Information Technology. This development has made accessibility to world facts and information possible from any phase of the globe. The huge development of computer networks changes to global cyberspace, the revolution of cyberspace changes the world's information streaming was very fast. People around the world can access many resources that they desire.

In the United States started with office machinery after that with revolution of technology office machinery had to upgrade to the modern computer in 1946. In 1970, the microprocessor technology changed the heavy computer to personal and business computer to compute the data and use widely. The videotext system to TCP/ IP (internet protocol) internet. In the 21st century, the huge development of ICT sector in the worldwide and the digital earth connectivity sector is increasingly developing, people can easily get information from another part of the globe and people can get the data in real time. The world is changed to a village by the revolution of the ICT Sector.

ICT has revolutionized the services mechanism of the global. The services offered manually and locally were disappeared in favour of online services with the

help of computer and internet technology. World the traditional modes of the business had changed to online business. With the development of ICT, people are relying on ICT technology in everyday of life and business. Almost all business and related work can be done over the internet such as shopping, mailing, banking, education, and communication.

In line with the revolution of ICT, the scope of cyberspace getting wider and wider. According to Bussell (2013), the cyberspace means, amorphous, supposedly "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's infrastructure.

The evolution and development of cyberspace into many daily lifestyle variables has contributed to the creation of the new information society concept as it offers fantastic opportunities. Unhindered accessibility can support democracy, because the flow of information is kept out of the authorities' hands, internet banking and shopping, utilization of mobile phone data services and voice over internet protocol (VOIP) telephony, these are some examples of how much involve of ICTs into people everyday lives and E-mails have taken place instead of conventional letters, for businesses, internet-based representation is now more essential than printed advertising materials and Internet-based networking and telephone services are developing more quickly than landline communications (Desai, 2020). The growth of ICT and improvement of cyberspace gives human beings the advantages and disadvantages of social economic life. According to Vapulus (2018) described the advantage and disadvantage of cyberspace were as follow;

The Advantages of Cyberspace are;

1. **Information Resource:** The Internet is a virtual information library. Any topic that people want can be searched, and it will be available on the Web. Google, other search engines and Yahoo are available and accessible for people service 24 hours a day, seven days a week. In real-time, we can get world details or current exchange rates.

2. **Communication:** It was difficult in the past to get in contact with anyone in a timely manner. Now we can connect with each other in the digital age of the Internet, such as text & voice messages or email and video calls.

3. **Entertainment:** These are some of the reasons why many people want to use the Internet is entertainment. For gaming and music, we can download new games. There are many games and music available for free download. The online gaming systems and gaming equipment businesses have expanded rapidly. Facebook, Twitter, and Instagram are used for entertainment by people. To connect with their followers, celebrities use the resources of the Internet.

4. **Social Networking:** Social networks in the network often play a significant role. Without Facebook or Twitter, we can't imagine life. It is now popular among people at the modern digital age and can change physical networks around the globe to communicate between each other. It has emerged as a remarkable platform for interacting with millions of people of common interests.

5. **Opportunity:** People can also look for business opportunities in the workplace, learning opportunities, forums, groups, and more, in addition to looking for lost friends. There are chat rooms, in addition, where users can meet new and interesting persons. Some will find a life partner for them.

Disadvantages of Cyberspace are;

1. **Security:** If people have access to internet banking, social networks, or other services the internet users' name, address, bank account & credit card information and sensitive personal information & data can be stolen. Then, cybercriminals use internet user's profile information to their benefit.

2. **Virus attack:** Internet users often suffer from virus attacks on their systems. Virus programs are started if people click on a malicious link. Internet connected computers are exposed to highly targeted virus attacks and may eventually be broken.

3. **Cybercriminal:** The capacity to send and receive emails has also, unfortunately, emerged as a method of distributing spam and malicious software to cybercriminals. Hidden Malware embedded email attachments

can wreak havoc on internet users' computers and may steal personal data. Cybercriminals used email as a means of attracting victims to reveal sensitive data, to deceive emotions.

On the other side of the ICT revolution and development, the Black Hand emerging is cybercrime due to the abuse and misuse of computer systems. Nowadays, modern people are daily using internet and ICT technology equipment, the more using the internet, the higher risk of being cyber-victims such as cyberbullying, cyber harassment stealing information and data via the modern technology. Cybercriminals are using several ways of technology to attack the victims, cybercrime is totally anonymous, it is difficult to trace out who committed.

2.4 Evolution of Cybercrime

As computer systems have become an important part of the day-to-day running of businesses, organizations, governments, and individuals, they are heavily rely on computer systems. As the result, people stored on their devices very important and valuable information. History has shown that important things are always targeted by criminals. People are using personal computers, phones, and more in daily life. The criminals were target to these important data for the benefit then commit the criminal activities.

In the past, in order to get access to a person’s valuables data for a criminal, the criminal would commit theft in some form or form. In the case of data theft, the criminal would enter a building by finding the files to commit data theft. In today’s world, criminals can attack their victims from afar because of the Internet nature (Staff, 2018). Regarding to the evolution of cybercrime with the improvement of computers and technology, Mujovic' (2018) described as the following table (2.1).

Table (2.1) Cybercrimes by Cases and Types

Year	Developer Name	Evolution of Cybercrime Cases	Type of Cybercrime
1971	John Draper	Phone Phreak	Fraud
1981	Ian Murphy	He hacked into the AT&T network and changed the internal clock to charge off-hours rates at peak times	Hacking
1982	Elk Cloner	Virus (It attacked Apple II operating systems and spread by floppy disk)	Virus
1988	Robert T. Morris jr	Worm Virus (infected over 600,000 operating systems and network)	Virus
1989	Unknown Developer	The very first massive ransomware case	Ransomware
1990	The Legion Of Doom and Masters Of Deception	Hacked into computers system and stealing data & hacks into telephone mainframe infrastructure	Hacking / Fraud
1993	Kevin Poulson	All the phone lines going to the LA radio station were controlled by him.	Hacking
1994	UK Student	Stealing information nuclear program of Korea, NASA and other US agencies	Hacking
1995	Unknown Developer	Macro-viruses are viruses written in application-integrated computer languages	Virus
1999	Unknown Developer	The Melissa virus was an email-based macro-virus with the intent of getting control of email accounts and sending with mass emails.	Virus
2000	Unknown Developer	Yahoo, EBay and many others were attacked by DDoS	Denial of Service (DDoS) attacks
2003	Unknown Developer	SQL Slammer Worm Virus (infection speed, it spreading out across nearly 75, 000 machines in within 10 minutes.	Virus
2007	Unknown Developer	Hacking, and malware, data theft infections	Hacking / Virus and Identify Theft

Source: https://www.le-vpn.com (Mujovic', 2018)

Table (2.1) described that the revolution of cybercrimes with the improvement of ICT sectors. Every year, technology is always improving so that the cybercriminal constantly developing new modern attacks to meet with the updated technology trends.

In 1971, John Draper committed fraud case by Phone Phreak attack, then with the development of telecommunication sectors in 1981, Ian Murphy committed the hacking case to AT&T network. In 1982, Elk Cloner developed a virus and attacked Apple II operation system, in 1988 the worm virus that created by Robert T. Morris jr, attacked with Worm Virus, it infected over 600,000 operating systems and network). 1989, Ransomware attacked emerged. In 1990, The Legion of Doom and Masters of Deception, they hacked telecom mainframe infrastructure and committed hacking & fraud cases. In 1993, Kevin Poulson hacked the radio station of LA, in 1994, UK student hacked and stealing information from the nuclear program of Korea, NASA and other US agencies. In 1995, (Macro-viruses) virus embedded application emerged. In 1999, The Melissa Virus appeared and attacked email account. In year 2000, DDos attacked to Yahoo, EBay and in 2003, SQL Slammer Worm Virus spread across nearly 75, 000 machines within 10 minutes. In 2007, the attacker developed a powerful attack that includes hacking attacks, data theft and malware infections to computers system and networks.

After 2010, the huge technology improvement was lead to commit cybercrime in many different ways and cybercriminals used a variety of technology, because of the raising of the social networks, online bank transition, storing information & data. A lot of people around the world are relying on the internet and modern devices, the internet, and ICT- related equipment are beings apart of human daily life so that people more using modern technology, they have more chance to be victims.

Cybercrime impacts society in several different ways: identity theft, cyberbullying, cyber abuse, phishing. The cybercrime fallout can have a lasting effect on life. A common technique used by scammers is forging, sending fraudulent emails that are supposed to arrive asking for personal information from banks or other financial institutions. If this information is given by internet users, it will allow criminals to access banks' accounts and credits, as well as open new accounts and breach the level of credit. Every year, intimately one percent of the world's GDP is lost by cybercrimes (Lewis, 2018).

The financial sectors are targeted by cybercriminals. Most of the financial sectors rely on digital networks for their businesses, these digital networks increase the risk of cybercrime. Cybercriminals are focusing on attacks, whether big or small. For their own purposes, hackers may take over company servers and steal data or attempt to use computers. Companies need to upgrade their software to hire employees and

prevent intruders. Therefore the business needs to spend more costs on cybersecurity (Khan, 2019).

2.5 Impact of Cybercrimes

Cybercrime also has an effect on mental and physical problems because based on physical attacks, rumors, and exclusions, cyberbullying can reach more people through social networking sites and other technology, and the victim cannot easily escape the bullies. Physiological symptoms are encountered by the cyberbullying victims. They report frequent headaches and stomach pain, often related to nervousness. They also can tend to self-harm, including with razor blades cutting or scratching their skin (Duverge, 2015). According to Knapton (2018), "Youths who have encountered cyberbullying, such as cutting, attempting suicide, and committing suicide, have been involved in self-harm. Cyberbullying makes young people more than twice as likely to commit suicide or self-harm".

Since the internet and social media are easily available to more and more people, cyber abuse against women and girls is an increasing issue. "Women are more prone to suffer extreme forms of cyber abuse than men, and the effect on their lives is even more traumatic" said Jurgita Peciuriene, EIGE's programme coordinator for gender-based violence (Peciuriene, 2017). Cyber harassment can have a major mental effect on people. Victims report a number of severe consequences of victimization including increased suicide attempts, fear, frustration, depression, etc (Kumar & Rajan, 2018). Cyberbullying and cyber harassment also impact on victims with long term problem in whole life.

i. Health Impact

According to MacKenzie, McEwan, Pathé, James, & Mullen (2011), cybercrime effects on victim's mental health. The victim starts feeling denial, confusion, self-doubt, questioning if what is happening is unreasonable, wondering if they are over-reacting, frustration, guilt, feeling embarrassment, self-blame in every manner, apprehension, fear, terror of being alone or that they, others or pets will be harmed, feeling empty and helpless to end harassment, depression, anxiety, suicidal thoughts, agoraphobia, depression (all symptoms linked to depression) (frightened to leave the house, never feeling safe in life), nightmares, ruminating, irritability, frustration, homicidal thoughts, emotional numbness and difficulty focusing, attending

and remembering things, inability to sleep finally suicidal thoughts and/or suicide attempts.

MacKenzie et al. (2011) pointed out cybercrime's impact on physical health Exhaustion from sleeping trouble, depressive symptoms, effects of chronic stress like headaches, hypertension Gastrointestinal problems, weight changes due to not eating or eating comfort development, or increased incidence of diseases pre-existing, for example, asthma, gastric ulcers, and psoriasis, dizziness, shortness of breath, increased use of alcohol, cigarettes or medications have an effect on health.

ii. Impact on Victim's Social Life, Work and School

Cybercrimes also effect on the victim's the social life, work and school. In the victim's social life, insecurity and lack of ability to trust others that affect current and future relationships and friendships, physical and emotional intimacy issues, avoidance of usual activities such as going to the gym, going out. Isolation, feeling misunderstood or psychological symptoms (Kumar & Rajan, 2018).The effect of cybercrime on work and school is declining school/work results, rising sick leave, leaving work or being fired, and changing professions, school dropout, poorer education and opportunities for careers (MacKenzie et al.,2011).

iii. Impact on Victim's Economy

Cybercrime has a negative effect on victims' income. When the victims suffered the cybercrimes, the victims will be financial losses regarding online fraud, then also impact on income loss. Effect of cyberbullying the victims can leave jobs, or changing professional and increasing medical leave and medical cost. If the victims reported to the police , the costs of the consequences were legal fees, the cost of increasing home and personal protection, the cost of repairing damage to property, receiving psychological counseling and medical treatment, the cost of breaching leases on leased property, and the cost of relocating (MacKenzie et al., 2011).

2.6 Basic Cybercrimes Awareness for Internet Users

Awareness is an initial step for a situation or fact to be recognized, understood, or known, and perception makes a difference about how to deal with it. To avoid being cyber victims, it depends on what the internet users know about cybercrimes and what are safe practices while using online. If the internet user has lacked both knowledge and

practices this internet user has a high risk to be cyber victims. Regarding the basic cybercrimes awareness, the internet user should know cybercrime's characteristic and before using the internet services. The internet users should have basics awareness of cybercrimes. In order to get cybercrimes awareness, the internet users should attend related cybercrimes awareness training or campaigns first. The basic cybercrimes awareness were as follows (Lee, H & Lim, H. 2019);

1. While using the internet services the internet users should not relate closely with the stranger on online.
2. Using all in one password cannot be safe information and privacy, password leaking were related with cybercrimes and difficult to control.
3. To avoid using crack & patch software, if using crack & patch software can be lead to virus infection.
4. While using bank transition, it should be used by private internet (mobile data or personal Wi-Fi).
5. Password leaking can occur by clicking the internet link that someone shares or sends.
6. Sharing information on chat rooms or social media can lead to cybercrimes such as cyberbullying, hacking, fraud, etc.

2.7 Review on Previous studies

The empirical studies on cybercrime in Myanmar is very rare. Thus, it can be reviewed on the international research paper. Regarding to the awareness of cybercrime, Muhammad Abdullah Avais, Wassan, Narejo & Khan (2014) examined on "Awareness Regarding Cyber Victimization among Students of University of Sindh, JamsHoro". They did the quantitative analysis with 100 respondents. They found that 57% of respondents were highly active on the internet and used more than 06 hours on various social networking sites. 39 percent of respondents spent 03-05 hours and 4 percent of respondents on social media sites spent less than 02 hours. 49 percent of respondents were extremely involved in chat rooms, with 37 percent of these respondents at high risk of becoming cyber victims in cyber communities due to contact with strangers. 37 percent of respondents spent 03-05 hours in chat rooms and 14 percent spent at least 02 hours a day, 53 percent of these respondents communicated in

the chat room with unknown people. 46% of respondents have suffered from phishing attacks. 44% of respondents did not face this assault because they never responded to emails from these phishing attacks or knew about these emails and viewed these mails as spam. 10% of respondents do not know about these types of phishing emails. 40 percent of respondents got bullying notifications for cyberbullying, 60 percent received flaming words either through emails or in public/private chat groups. 82% of respondents thought that women were prone to cyber-attacks on the internet, while 18% felt that there was no chance of cyber-attacks on women.

In addition, Sreehari, Abinanth, Sujith, Unnikuttan & Jayashree (2018) studied on awareness of Cybercrime among College Students with Special Reference to Kochi. They pointed out the rise in cybercrime in INDIA problems such as lack of proper cyber-related training and education, weak level of cybercrime awareness among Indians were the main factors to the growth of cybercrime. INDIA's law enforcement has faced huge problem problems in tackling cybercrimes due to the high rate of cybercrime. They found that 25.1% of respondents were very aware about cybercrime. 51.7% know about cybercrime. 21.7% don't know very well about cybercrime, while only 1.4% doesn't know anything about cybercrime.

Regarding cyberbullying, Soe Hay Mar Oo (2019) studied the effect of Social Media on Students' Life". She found that 56% of the respondents mostly used social media for the professional and career development and perceived as improvement tool for academic performance by 35% of the students. Her studied pointed out that all of people are using social media for their carrier or their academic development, some percentage of respondents were using social media for their relaxing, assumption in her studied all of respondent using social medial. She found that the respondents have cyberbullying experienced when using social media. It was found that total 116 (75.3%) of respondents have never experienced cyberbullying and 36 (23.4%) have experienced often. Only 2 (1.3%) have always experienced.

CHAPTER III

ICT AND CYBERCRIMES IN MYANMAR

3.1 Development of ICT Infrastructures in Myanmar

The world today has become globalization because of the improvement of ICT around the globe. The people around the world are applying inexhaustible modern resources of information and communication technology (ICT). The ICT sector of Myanmar is still upgrading to be able to keep abreast of word Information Communication and Technology.

Formerly, Myanmar lagged behind in the development of the communication sector. In Myanmar, there had post offices and telegraph offices for communication facilities. So that People in Myanmar had accessed the poor communication. For the sending a letter, it took for a long time, too many weeks from one place to another. People who lived in a remote area were difficult to access these communication services. Until 1988, in Myanmar, many major towns relied on magneto telephone. Information technology in advance a leaps and bond in the late 20^{Th} Century and early 21^{Th} century. In creating a new life style of the Myanmar human society that occurred after 1988, progress ICT helps shape of new nation. The ICT infrastructure, the critical basic foundation of telecommunication as well as e-commerce, e-government and e-learning. Without the adequate ICT infrastructure, the ICT sector will not be achieved the goal (Thinn Thinn Aye, 2012).

There are institutions in Myanmar ICT development, Myanmar computer Science Development Council is established in 1996.Myanmar Computer Federation (MCF) is established in 1988. MCPA (Myanmar Computer Professionals Association), MCIA (Myanmar Computer Industry Association), and MCEA are subordinated by MCF (Myanmar Computer Federation) (Thinn Thinn Aye, 2012).The evolution of ICT infrastructure can be summarized by table (3.1).

Table (3.1) Evolution of ICT Infrastructure in Myanmar

Year	Myanmar ICT infrastructure Development
1990	Domestic satellite system (SCPC) was established for remote and border area
1993	Cellular mobile phone system (Analogue APMS 800) was established
1994	The International and National Electronic Transit Switch and the Standard A satellite earth station have been developed.
1995	WLL (Wireless Local Loop) was introduced.
1996	Digital AMPS cellular system and DECT radio telephone system have been presented.
1997	SEA-ME-WE 3 submarine cable system, X.25 e-mail system and CDMA cellular system were introduced
1998	VAST system of domestic communication was established for remote and border area.
1999	Dial-up access system for internet and e-mail was established.
2001	GSM cellular system has been launched
2004	The Advance Communication Project was launched and the project consisted of an IP satellite communication system, a VoIP system, and a data communication system.
2005	ADSL and optical internet and e-mail access systems have been established.
2006	New international and national electronic transit switches have been established. The FTTP access system has been introduced.
2007	The domestic satellite system (SCPC) has been terminated. The GMS project was introduced and included Digital-Switches, optical fiber transmission system, microwave transmission system, Soft-switch, trunk gateways, access gateways, IP metro network, CATV system.
2008	National Gateway for Internet and IXP was established. Myanmar-China cross border optical fiber link, Myanmar-Thailand cross border optical fiber link, Myanmar-India cross border optical fiber link was commissioned.
2009	WCDMA and McWill broadband wireless access system was introduced

Source: Sai Saw Lin Tun (2014), available at https://www.unescap.org

Due to installation of auto-telephones and mobile telephones, 1.92 telephones ratio to 1000 people in 1988 increased to 39.95 for 1000 people in the year of 2010. There were 74,855 ordinary telephones lines in 1988, number of telephone lines reached 229,741 in September 2010. In addition to improving communication sector in the urban areas, the PCO-Public Call Offices have been installed in States and Regions for uplifting the communication sector of rural people in accord with the guidance of

the Head of State. Use of CDMA-450 system mobile phones commenced in Nay Pyi Taw in June 2009. CDMA450 (PCOs) were constructed in wards and villages surrounding Nay Pyi Taw beginning 2010. PCOs across the nation have been installed with GSMs and CDMA-450 mobile phones. MPT Satellite Terminal project was implemented in cooperation with Thailand with the aim of enabling the far-flung areas and poor transport areas of States and Regions and border regions to have easy access to better communication and enjoy development fruits of social, economic and health sectors. As a result, the remote and far-flung areas across the nation have easy access to telephone, fax and Internet through MPT Satellite Terminals. On 16-7-2004, GSM mobile system was implemented for creation of better communication system among Yangon, Mandalay and other major towns. Therefore, the residents of these areas can use new mobile phone system to make calls to any part of the nation and can apply advanced communication technology in connection with other countries through Internet. During about two decades, new facilities of communication sector have uplifted the living standard of the people. Significant progress can be seen in social, education, economic and health sectors (Zaw Moe Thauk, 2010).

3.1.1 Development of Telecommunication in Myanmar After 2010

According to Nam, Cham & Halili (2015), MPT has been controlled for many years as a monopoly provider of mobile and fixed telecommunications services. According to Deloitte Southeast Asia 2013 report, in 2012, MPT had 14,000 kilometers of fiber optics and about 1,800 towers connect Myanmar, 80 percent of this infrastructure is owned by the military, with the MPT owning the rest, Just a few companies offer Internet services that were only launched in Myanmar in 1999: MPT, the public company Yatanarpon Teleport, and the privately-held Red Link Communications, SkyNet, and other providers of Fiber to The Home. ICT services are still mainly under the government's control.Until around 2012, telecommunications were exclusively controlled by the Myanmar Post and Telecommunications (MPT). The company's monopoly on the quality of telecommunications was extremely low, and even if one could connect, the quality of voice was so poor that it was sometimes impossible to communicate. The low quality of the telecommunication service was a big issue in Myanmar doing business.

Telenor (Norway) and Ooredoo (Qatar) were licensed for operate on mobile operators in 2013 by the Myanmar government and KDDI (Japanese

telecommunications operator) start providing tech support to MPT. It brought significant changes in the system. Since then, investment in telecommunications infrastructure has arisen non-stop with international companies running Myanmar's telecommunications market, bringing substantial changes to the telecommunications sectors. Then a new SIM card selling for about 1500 Kyats came on the Myanmar's market in 2014, and almost anyone could buy one at this price. The number of subscribers totaled 1,243,619 while analyzing data in 2011, while the diffusion rate stood at 2.38 percent. However, by 2016, 8the number of subscribers had increased to 48,728,399, representing a colossal amount of growth, with the diffusion rate at 89.26 percent (Yangon Stock Exchange. n.d.).

Myanmar's fourth telecom provider, Mytel, was issued an operating license on 2017. The interest in mobile phones continues with the introducing of high-end mobile signal services and new mobile phone models, and the utilization rate of mobile devices has spread rapidly and it is now an important part of everyday life. Mobile phone coverage is also expanding and now covers all major domestic areas. Telecommunications have been more reliable in terms of efficiency and the business's usage has also significantly improved.

As the improvement of mobile SIM card users around the country and also mobile and internet financial services have developed, the new cybercrimes are committed by unregistered SIM card numbers so that Myanmar's Government encouraged to SIMs cards users to do register on respective operators. According to the data portal website, in 2020 Myanmar mobile phone users are 68.24 million (126% of Myanmar total population 54.3 Million).

3.1.2 Internet Development in Myanmar

Internet in Myanmar began to open up to the public in 1998-1999 when the government-controlled Myanmar Post and Telecommunication (MPT) signed an agreement with the American Company Eagle that allowed Eagle to introduce an email service to the general public (Erin, 2016). In 2010, internet penetration in Myanmar was less than 0.3 per cent of the population, amounting to a mere 130,000 users (Shadrach, 2018).After 2013, the SIM card prices felled to 1.5$ (1500 Kyats) so that mobile subscriber rate in Myanmar is rising rapidly. According to James (2019), in 2019 Myanmar’s SIM card penetration rate was over 105%.Then Myanmar internet user rate were rapidly high after 2014. As the arrival of cheap Chinese-made

smartphones and SIM cards mobile Internet access in Myanmar raising up internet population. Even Myanmar People who live in remote areas can access 2G service, 3G, and 4G internet connections. According to Yangon Stock Exchange. (n.d.), in 2015, a total of twenty-two companies have received wired, wireless, and telecommunications infrastructure licenses, accompanied by 19 more licensed companies in 2016 and 10 extra in 2017, bringing the current total to fifty-one companies retaining internet licenses. As of 12 December 2017, there have been 137 companies providing internet related services in Myanmar, which includes four cellular phone companies and all other kinds of telecommunications-related businesses.

As the number of internet service providers increases, internet services' competitive market was developed. So that the internet services provider provides their best to customers, such as top-up bonus, data package bonus and high-speed internet. Now Myanmar people have much of choose the best services not only mobile internet but also wireless broadband and fiber-optic internet. With the plenty of services provider and high-speed internet, Myanmar people rely on the internet for their daily business. The people are using internet by many different desires such as shopping, education, promotion on social media, chatting, emailing, gaming and entertainment, etc. The proliferation of mobile internet and social media in Myanmar has created jobs, increased foreign investment, and connected millions of people.

Table (3.2) Development of Internet Users in Myanmar (2010-2020)

Year	**Internet Users (Million)**
2010	0.1
2011	0.5
2012	0.5
2013	0.8
2014	1.1
2015	1.2
2016	1.3
2017	14
2018	18
2019	21
2020	22

Source: https://www.internetlivestats.com & https://datareportal.com

Table (3.2) described that the development status of internet users in Myanmar. In 2010 there have only 0.1 million internet users in Myanmar. In 2013 the Myanmar Telecommunication sector reform and private sector participation were started the foreign investment telecom companies Telenor and Ooredoo are started to implement their telecom infrastructure and KDDI (Japanese telecommunications operator) provided the technical support to MPT to improve connectivity. After 2014, the operation of Foreign telecom companies, these companies provide 3G, 4G internet so that after 2014 Myanmar internet users were started raising, then in 2017 Mytel telecom company invested in telecommunication sectors, starting from 2017 Myanmar internet users population were rapidly high. In 2020 total Myanmar internet users were 22 million.

3.2 Rules and Regulations of ICT In Myanmar

Rules and regulatory framework play a vital role to promote and to develop the ICT sector. The legal framework concentrates not only on the current status but also on future steps and long-term policies. In Myanmar, there have no separate enacted laws for cybercrimes but to develop of the ICT sector and society, Myanmar enacted Computer Science Development Law (1996), Electronic Transaction Law (2004), and Telecommunications Law (2013).

According to Myanmar Law Information System. (n.d.), there are three ICT and cyber related laws in Myanmar. These are, Computer Science Development Law (1996), this law was enacted by The State Law and Order Restoration Council Law No. 10/96 on 20th September 1996. The Electronic Transactions Law (2004), this law was enacted by The State Peace and Development Council Law No. 5/2004 on 30th April, 2004. The Telecommunications Law (2013), this law was enacted by The Pyidaungsu Hluttaw Law No. 31, 2013 on 8th October 2013.

Regarding the cybercrime there have two enacted laws were taking action to cybercriminals, these are the **Electronic Transactions Law** (2004) and **The Telecommunications Law** (2013). **The Electronic Transactions Law** (2004) section (34) enacted about Cybercrime Case, whoever commits any of the following acts shall, on conviction be punished with imprisonment for a term which may extend to 5 years or with fine or with both:

(a) sending, hacking, modifying, altering, destroying, stealing, or causing loss and damage to the electronic record, electronic data message, or the whole or part of the computer programme dishonestly;
(b) intercepting of any communication within the computer network, using or giving access to any person of any fact in any communication without the permission of the originator and the addressee;
(c) communicating to any other person directly or indirectly with a security number, password or electronic signature of any person without permission or consent of such person;
(d) creating, modifying, or altering of information or distributing of information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organization or any person.

The Telecommunications Law (2013), in section (66), it also enacted for cybercrime case, whoever commits any of the following acts shall, on conviction, be punished with imprisonment for a term not exceeding three years or with fine or with both:

(a) accessing and disturbing the telecommunications network, altering or destroying the determination of technical standards or the original form without the permission of the owner or a person who has the administrative rights.
(b) releasing a virus or using any other means with an intention to cause damage to the telecommunications network.
(c) stealing, cheating misappropriating or mischief of any money and property by using any telecommunications network.
(d) extorting, coercing, restraining wrongfully, defaming, disturbing, causing undue influence or threatening to any person by using any telecommunications network.

The Electronic Transactions Law (2004), in this law section 34 is the law to take action for related cybercrimes cases. Section 34 (a) is the act that to take action for especially hacking cases, such as data hacking, data modifying, aim to lose or damage data. Section 34 (b) can be taking action on Hacking cases relating to computer system hacking and security permission hacking. Section 34 (c) can take the action for the

criminal who commits the Identify Theft case, especially for password-stealing cases. Section 34 (d) is to take action to the criminal who commits cyber harassment cases such as posting an inappropriate website with Photoshop editing photos to be lower the dignity of any person or organization.

The Telecommunications Law (2013), at that law section 66 is to take action for related cybercrimes cases but not cover for all cybercrimes cases. In this laws section (66D) is the most prominent related cybercrimes law in Myanmar .Section 66 (a) is to punish for the cybercriminal who commit hacking through from every communication networks. Section 66 (b) is to take action for virus cases. Section 66 (c) is to taking action for fraud cases. Section 66 (d) is especially taking action for cyberbullying cases but it is used to take action for online defaming to the government. This 66 (d) can also take action for fake accounts and spreading fake news on social media or other internet platforms.

Overview to The Electronic Transactions Law (2004), section 34 can take action for Hacking, Identify theft, cyber harassment. The Telecommunication Laws (2013) also to take action for Hacking, for fraud, cyberbullying and virus. Myanmar does not have any specific law to protect data privacy but the data is not completely unprotected (Daniels, 2017). There has a lack of specific rules and regulations regarding cybercrimes and cybersecurity these laws were not full coverage of all cybercrimes cases such as data protection, child online protection, and critical infrastructure protection, etc. And then also weak in law enforcement because technicians still needed in respective departments (Ye Naing Moe, 2018).

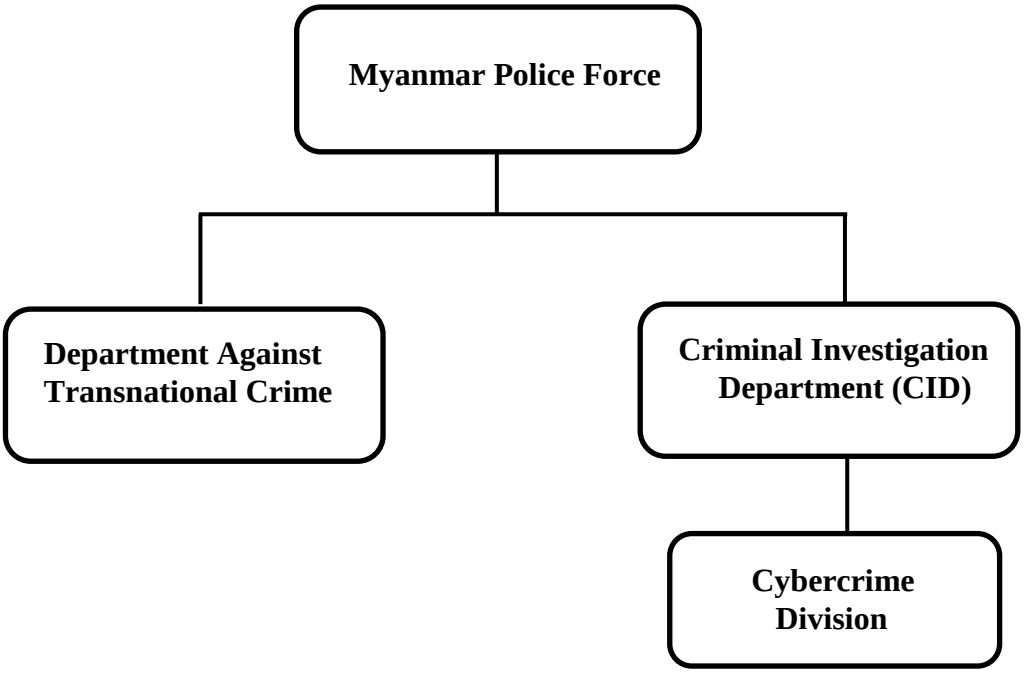
3.2.1 Organizational Structure of Myanmar Cybercrime Division

According to ASEANAPOL. (n.d.), the British policing system was introduced in 1885 when the Union of Myanmar became a British Colony. At that time, the Police Force was known as the Burma Police. The Burma Police was reorganized as the People's Police Force in 1964 and was reorganized again to the present set-up as the Myanmar Police Force on 1st October 1995.Myanmar is one of the member states of the United Nations. The Myanmar police force carried out its contribution in accordance with UN Security Council Resolutions 1373, 1276, and 1455. Myanmar has been a member state in the United Nations Convention against Transnational Organize Crime on 30 March 2004. As a result, the Myanmar police force was originally established transnational criminal unit in September 2004. The Department of

Transitional crimes cooperation with internationally, neighboring ASEAN and Asian countries. The following crimes are mainly eradicated: (a) terrorism, (b) drug crimes, (c) arms smuggling, (d) piracy, (e) cybercrime, (f) money laundering, (g) human trafficking, (h) economic crime. The Cybercrime Division was established under the Criminal Investigation Department in 2015 (Structure of Myanmar cybercrime divisions Show in figure 3.1) and it has been taking actions and assisting cybercrime in Myanmar country since today.

According to ASEANAPOL. (n.d.), Myanmar was a member of INTERPOL (International Criminal Police Organization) and cooperated in the field of police work with INTEROL headquarters and among member countries, exchanges of news on crimes, seminars, training courses and crime prevention programs on cross-border crimes. The Cyber Crime Unit has been set up and expanded to prevent and expose cases of defamations, fraud, theft of news and information, threats and harassment on Internet social networks. As the interconnection and relationship with INTERPOL and ASEANAPOL have increased and developed, the organization and structure of the Myanmar Police Force has been expanded and modernized in line with the modern age. In Myanmar cybercrimes division there have mobile Computer Forensics and Mobile Device Forensics to investigate and trace out cybercrimes related cases.

Chart (3.1) Organizational Structure Myanmar Cybercrime Division



Source: https://rm.coe.int/03-myanmar-presentation/168072bd20

In Myanmar cybercrimes division there have mobile Computer Forensics and Mobile Device Forensics to investigate and trace out cybercrimes related cases. According to Ye Naing Moe (2018), he pointed out that to investigate the cybercrimes cases the technician were still needed for respective departments and specific guidelines were also need to take action on cybercrimes.

3.3 Cyber Security and Cybercrime Awareness Organizations in Myanmar

Cybercrime and cybersecurity risks are increasing day by day because they are driven by global connectivity and the use of internet services. Cyber threats can come from any Internet source at any level of organization. Cybercrimes are linked to human life, to the economy, and to a huge impact on our society. Nowadays, everyone needs to know about cybercrime and cybersecurity, what cybercrime threats are, what potential impacts cyber-attacks will have on business, the economy, mental and physical health. To provide awareness-raising training and campaigning, it may be difficult for only government organizations to do so, which are needed for additional technical and financial support from other organizations, such as (NGO, INGOs). In Myanmar, cybersecurity and cyber-crime awareness organizations are supporting government activities and campaigns.

According to mmCERT (2020) official website, Myanmar Computer Emergency Response Team (mmCERT) was formed by e-National Task Force on 23 July 2004. mmCERT/cc was launched by Ministry of Communication and Information Technology on 15 December 2010.mmCERT, a national CERT in Myanmar is a non-profit organization for dealing with cybersecurity incidents across an organization. mmCERT is a national computer emergency response team for dealing with cybersecurity incidents in Myanmar. Besides doing incident handling activities mmCERT works to increase public awareness in cybersecurity and supports technical advisories in its community. Besides doing incident handling mmCERT also works to increase public awareness in security with the various ways of resources sharing to our community. And it intends to provide cybersecurity advice to Myanmar Internet users to prevent Internet based attacks. mmCERT provided the following services;

(1) Incident Handling: Handle the cyber-security incidents promptly depending on the efficient working mechanism with the carriers, domain registrars and security vendors as well as on the close cooperation mechanism with vital information departments and enforcements.

(2) Latest Threats and Security News Sharing: Handle the cyber-security incidents promptly depending on the efficient working mechanism with the carriers, domain registrars and security vendors as well as on the close cooperation mechanism with vital information departments and enforcements.

(3) Technical Advisory Support: Handle the cyber-security incidents promptly depending on the efficient working mechanism with the carriers, domain registrars, and security vendors as well as on the close cooperation mechanism with vital information departments and enforcements.

(4) Public Awareness Promotion: Handle the cyber-security incidents promptly depending on the efficient working mechanism with the carriers, domain registrars, and security vendors as well as on the close cooperation mechanism with vital information departments and enforcements.

The Cyber Bay Kin [2] collaborates with Ministry of Transportation and Communication's National Cyber Security Centre especially to provide awareness and educational programs relating with cybercrimes awareness and cybersecurity in Myanmar.

3.4 Digital literacy in Myanmar

Digital literacy is a method regarding the ability to understand the processing of literal meanings, information and data. Digital Literacy refers to the ability to generate digital resources, new knowledge, and methods to properly identify, access, manage, integrate, value, quantify, analyze, and synthesize digital tools and features of consciousness, attitudes, and individuals. Create exhibitions and interact with others. In certain situations, engage in creative social work and think about pros and cons. So many more people are now coming online and connecting with friends, families and communities, and digital literacy has been more crucial than ever.

Digital literacy needs not only the skill to understand and use technology itself, but also the ability to think critically and assess digital knowledge from a wide variety

[2] Cyber Bay Kin, Founded in 2018 by U Ye Thura Thet and Lennon Chang, a lecturer in criminology at Monash University, Australia. Cyber Bay Kin was launched in cooperation with the Ministry of Transportation and Communication's National Cyber Security Centre, and is supported and funded by the Australian Department of Foreign Affairs and Trade as part of its International Cyber Engagement Strategy, and the university's School of Social Sciences (Saw Yi Nanda, 2019).

of sources. From banking to social media, from cloud software, within the 21st century, technology can continue to change a life. These skills will become a very important part of the cultural and economic success of the country as Myanmar becomes more integrated with the world economy (King, 2019). According to Ye Naing Moe (2018), in Myanmar, schools do not teach digital literacy skills and don't have a digital curriculum so that people in Myanmar were lack knowledge regarding digital technologies.

According to Telenor Myanmar (n.d) only 3% of Myanmar families owned computers, in comparison to an African and Asia-Pacific average of 9% and 36% respectively. In the unexpectedly developing and digitally interconnected Myanmar economic system where, in line with the Asian Development Bank, skilled labour is in short supply, the overall lack of professional computer digital literacy reduces employment possibilities for the huge majority of Myanmar's labour force while creating recruitment challenges for employers. Telenor Myanmar provided free digital literacy training via Telenor Digital School Program over a million students. From this free digital literacy training, the student obtained primary Microsoft Word, Excel, and PowerPoint, internet search, e mail and safe internet courses.

On 2019, with the collaboration of Ooredoo Myanmar and Google Asian Pacific provided a digital literacy and citizenship training program throughout Myanmar with the recognition of the Ministry of Education. In this training, they trained young Myanmar people approximately for secure internet using, digital empathies and responsibilities (Ooredoo Myanmar, 2019). The Inclusive Internet Index 2020 showed the status of ASEAN Countries Digital Literacy score. In this score Cambodia (46.9), Laos (47.6), Thailand (59.6), Philippines (63.9), Myanmar (65.1), Vietnam (70), Indonesia (71), Singapore (76.8), Malaysia (82.8), Brunei (No Data). According to this score, Myanmar is not too low skill in Asean Countries. Myanmar has higher digital skills than Cambodia, Laos, Thailand and the Philippines. (See in table 3.3)

Table (3.3) Asean Countries Digital Literacy Skills (2020)

Asean Countries Digital Literacy Skills	
Country	Score/100
Malaysia	82.8
Singapore	76.8
Indonesia	71
Vietnam	70
Myanmar	65.1
Philippines	63.9
Thailand	59.6
Laos	47.6
Cambodia	46.9
Brunei	N.A

Source:https://theinclusiveinternet.eiu.com

3.5 Cybercrimes Cases in Myanmar

The Internet has created borderless societies around the world, providing unprecedented possibilities to generate wealth and stimulate economies. Countries around the globe were seeking to take advantage of new technologies to foster economic growth and facilitate access to information and services. With the development of Internet services, the Black Hand emerge, it is called cybercrime. Cybercrime is one of the greatest challenges in every country in the world. Countries around the world seek to benefit from new technologies to drive economic growth and facilitate access to information and services. The development of mobile internet and social media in Myanmar has created jobs, increased employment opportunities, boosted international investment, and connected millions of people to a world of information and it introduced millions of young people. But it has also brought with it a dark side of cyber problems the country is not yet ready to tackle. As internet access in Myanmar expanded with affordable SIM cards, reliable 3G and 4G network infrastructure, and wireless broadband internet. Even the rural and remote areas in Myanmar can access mobile data internet. So that internet users are rapidly growth in Myanmar year by year.

The highlighted fraud case occurred in 2015, A BULGARIAN citizen Mr Milen Atanasov, he committed fraud by using fake ATM. He withdraws money from several Banks ATM machines. In 2016, a report of Telenor Myanmar about children are under threat of cyberbullying. Telenor Myanmar Surveyed 12,368 Telenor subscribers and

staff members. This survey found that 25 percent of the adult respondents said they had seen kids being cyber-bullied, and 23 percent of the children said they believed the issue was serious. The report also described that 11 percent of the child respondents have been cyberbullied or were familiar with underage victims of cyberbullying (The National Thailand, 2017). There are 137 cyberbullying cases in the reported cybercrimes in Myanmar in 2017 (Thaung Htwe & Kyaw Naing Latt, 2017).

According to the report of Achard (n.d), Department of Transnational Organization Crime, 2 case of cybercrime and on 2013 and 6 cases of cybercrimes in 2014. Table (3.4), described the number of cybercrimes cases that happened from 2013 to 2018. There were totally 50 cybercrimes reported cases in 2015 accordingly to the data of Myanmar Cyber police department. In 2016 the cybercrimes case were rise up to 300 cases. In 2017, reported cybercrimes case were 500 cases and 780 cybercrimes cases in 2018. Furthermore based on the official report in 2019, more cybercrime cases might have gone unreported and most cybercrimes cases reported are involved online fraud and online sexual violence. Other cybercrimes attacks to the government (hacking ministries' websites) and the spreading of hate speech concerning with Rakhine problem. This was done by cyber attackers with fake accounts and they make sure they're not traceable. But if the Myanmar Cyber Police know their location, the Cyber Police will coordinate with the local police trace them, and take action.

Table (3.4) Cybercrimes Cases in Myanmar (2013-2018)

Years	Cybercrimes Cases
2012	0
2013	2
2014	6
2015	50
2016	300
2017	550
2018	780

Source: https://www.interpol.int and https://rm.coe.int

Accordingly before 2013, cybercrime case was very rare in Myanmar due to the lack of technology developments in every sectors and Myanmar people cannot use the internet widely. After investing of the foreign telecoms companies in 2014, it makes huge development for Myanmar telecommunication and internet services, as the

development of telecommunication services and internet development Myanmar people can use phone communication and internet services around the country and business sectors in Myanmar had changed online platform especially banking sectors and people in Myanmar used social Media widely. Thus, the cybercrimes rates were rising extremely after 2015. Total cybercrimes cases that happened from 2013 and 2018 were 1688 cases. The types of cybercrimes that happened from 2013 to 2018 were shown as below Table (3.5).

Table (3.5) Types of Cybercrimes Cases in Myanmar (2013-2018)

Type Of Cybercrimes Cases	Cybercrimes Cases (2013-2018)
Hacking	87
Cyberbullying	374
Fraud	359
Phishing	66
Identify Theft	311
Ransomware	48
Cyber Harassment	443
Total	1688

Source: https://www.interpol.int and https://rm.coe.int

Table (3.5) described that types of cybercrimes cases that happen from 2013 to 2018. In total cases 1688 cybercrimes cases in Myanmar, the Cyber harassment and Fraud are higher than other cybercrime cases because, people in Myanmar don't have good knowledge and practices to prevent the cybercrimes and don't know about dark side social medias. Then the social Medias users were closely related with the strangers on online so that the cyber harassment and cyberbullying were high. The online fraud case was the second highest cases, because Myanmar people were start using internet baking, online shopping, wave money and other transition services. The people lack of knowledge on respective password security to use these online banking and online money transition services. Cyberbullying cases are the third place of cybercrime used to happen in Myanmar because people were sharing their information and private

information to social Medias and chat rooms, the consequence was cyberbullying cases were high. Cyber harassment, Fraud and cyberbullying cases are frequently occurred on social media such as Facebook, Instagram and web base chat room in Myanmar.

After the rapid increase of Internet services, as well as the growing vulnerability of Internet users in Myanmar, people are unaware of the risks online and how to protect themselves. Many people lack the knowledge to protect themselves from cybercriminals. It's a huge challenge because Myanmar's Internet penetration is expanding but there is a lack of cybersecurity knowledge.The possible risks of cybercrime are high in Myanmar because many people do not understand the fundamentals of this kind of crime and thus is easy to be exploited. In particular, Myanmar's banking sector needs strong protection because many people lack trust in online banking services and local lenders. This is an obstacle, not just to banks, but also to service providers. The lack of protection in the banking sector often leads to cybercrime threats occurring in the future (Thiha, 2017).

Unregistered SIM cards, these will be huge risks for Cybercrime in Myanmar, the criminals can use these unregistered SIM cards to commit cybercrimes cases. When Myanmar people buy their phones, many social media applications are usually pre-installed, Facebook applications will always be one of them. Many of Myanmar people have no skill to do social media account creation by themselves, so that they ask the other people to create a social media account, email account. When they get users' names and passwords for their accounts and accessing online services, they go to Facebook and usually stay there. They have no knowledge to change their password. A consequence of these social media accounts, many fraud cases, and many cybercrimes occurs more and more in Myanmar. Without cybersecurity and cybercrime awareness, the more potential cyberattack will be facing more and more in the future in Myanmar.

CHAPTER IV

ANALYSIS ON CYBERCRIME AWARENESS

4.1 Profile of Study Area

Yangon is the study area to analyze cybercrimes awareness. There have main 26 internet service providers companies these providers provided a variety of internet services such as Mobile Data internet, Wi-Fi broadband, Fiber internet and etc. The estimated population of internet users in Yangon is (3.7 million) 70 percent of the total population (5.3million). Yangon is the largest city in Myanmar. Yangon is not only a country financial center but also a trade and logistic hub. Yangon has the country's main airport and seaport. Yangon has the largest population in Myanmar, the people across the country come and work & stay in Yangon for their different purpose. Yangon has many foreign investments and many jobs opportunity. Many people come from various fields and different layers with dissimilar education levels. The improvement of Telecommunication and broadband services in Yangon changes people's lifestyles and daily work environments. With the development of the modern ICT lifestyle, Yangon is the highest cybercrimes rate than other cities.

4.2 Study Design

This study was used the descriptive method with the quantitative approach by using the snowball sampling method for data collection in order to examine the level of cybercrime awareness of Internet users in Yangon and identify the type of cybercrimes used to happen in Yangon. The data were collected via online surveys. A survey was conducted with structured questionnaires. This research was carried out with 1071 respondents who live in Yangon.

Regarding the questionnaire design, the questionnaire comprised six sections, section (1) as characteristic of respondents with four questions. Section (2) is the respondent’s usage of internet services with five questions. Section (3) is the cybercrimes knowledge section constructed with seven questions. Section (4) is the

actual practice questions with seven questions and section (5) is the regarding rule and regulation question constructed by two questions. Section (6) is the cybercrime experience questions with thirteen questions to analyze the cybercrimes awareness levels and type of cybercrimes used to happen in Yangon internet users.

4.3 Analysis on Survey Data

The data analysis conduct with the demographic information of respondents and followed by study-related detailed information to meet the study objectives. Each component of the study was presented and analyzed in the following accordingly.

4.3.1 Characteristics of Respondents

The study was conducted with 1071 (out of 1200) respondents who were internet users in Yangon. The respondents were different gender, ages, and education and occupations levels. In this survey, there were Male 381 and Female 690 of total respondents.

Table (4.1) Gender and Educational Distribution of the Respondents

Gender	Graduate	University	High School	Primary School	Total
Female	592 (55.28%)	95 (8.87%)	3 (0.28%)	0 (0.00%)	690 (64.43%)
Male	301 (28.10%)	59 (5.51%)	13 (1.21%)	8 (0.75%)	381 (35.57%)
Total	893 (83.38%)	154 (14.38%)	16 (1.49%)	8 (0.75%)	1071 (100%)

Source: Survey data, 2020

Table (4.1) showed that the number of respondents' gender and educational levels. For the female respondents, there were 592 (55.28%) graduate respondents, 95 (8.87%) female respondents were university level, 3 (0.28%) were high school levels and there had no primary school level respondents in female respondents. At the male respondents, 301 (28.10%) were graduate, 59 (5.51%) were university level, 13 (1.21%) were high school and 8 (0.75%) male respondents were primary level. In terms of educational classes, there were 893 (83.38%) Graduate respondents, 154 (14.38%) people in University, 16 (1.49%) respondents in High School and 8 (0.75%) respondents in Primary School. Accordingly, the highest number of respondents are graduate level and the least number of respondents were primary school level.

Table (4.2) Respondents' Occupations Types by Educational Classes

Education Classes	Number of Respondents' Occupations Types				Total
	Employees	Dependent	Self-Service	Student	
Graduate	705 (65.83%)	27 (2.52%)	100 (9.34%)	61 (5.69%)	893 (83.38%)
University	29 (2.71%)	0 (0.00%)	8 (0.75%)	117 (10.92%)	154 (14.38%)
High School	4 (0.27%)	1 (0.09%)	7 (0.65%)	4 (0.37%)	16 (1.49%)
Primary School	4 (0.37%)	0 (0.00%)	1 (0.09%)	3 (0.28%)	8 (0.75%)
Total	742 (69.28%)	28 (2.61%)	116 (10.83%)	185 (17.27%)	1071 (100%)

Source: Survey data, 2020

Table (4.2) described the respondents' occupation types by educational levels, it was found that the total number of employees were 742 (69.28%), total number of dependents respondents was 28 (2.61%), the total number of Self-Services respondents were 116 (10.83%) and the total number of students was 185 (17.27%). Among the respondents' occupations, employee respondents were the highest number in total 1071 respondents.

Table (4.3) Daily Internet Usage Time by Respondents' Education Levels

Educational Classes	Daily Internet Usage Times (Hour)				Total
	1 to 5	6 to 10	11 to 15	More than 16	
Graduate	**464 (43.32%)**	317 (29.60%)	82 (7.66%)	30 (2.80%)	**893 (83.38%)**
University	80 (7.47%)	57 (5.32%)	13 (1.21%)	4 (0.37%)	154 (14.38%)
High School	13 (1.21%)	3 (0.28%)	0 (0.00%)	0 (0.00%)	16 (1.49%)
Primary School	1 (0.09%)	3 (0.28%)	4 (0.37%)	0 (0.00%)	8 (0.75%)
Total	**558 (52.10%)**	380 (35.48%)	99 (9.24%)	34 (3.17%)	1071 (100%)

Source: Survey data, 2020

Table (4.3) showed that respondents' daily internet usage times by different educational classes. It was categorized into four categories. These were, 1 to 5 hours, 6 to 10 hours, 11 to 15 hours, and more than 16 hours. The survey data have shown that 558 respondents were mostly used the internet for (1 to 5) hours in a day. It is highest

which has 52.10% of total respondents and the majority are graduate level. Some (2.8%) use the internet more than 16 hours a day which is the longest internet usage time in a day. Undergrad level can also use the internet for (1 to 5) hours in a day.

Table (4.4) Types of Email Usage by Respondents (Gender)

Email Types	Male	Female	Total
Personal	139 (12.98%)	286 (26.70%)	425 (39.68%)
Office	19 (1.77%)	58 (5.42%)	77 (7.19%)
Personal & Office	**184 (17.18%)**	287 (26.80%)	**471 (49.98%)**
Not Using	39 (3.64%)	59 (5.51%)	98 (9.15%)
Total	381 (35.57%)	690 (64.43%)	1071 (100%)

Source: Survey data, 2020

According to the above table (4.4), the types of email usages can be categorized into four types; personal, office, personal & office, not using email. These data showed that only total personal email users respondents percentage were 425 (39.68%), total office email utilized respondents were 77 (7.19%), using both personal & office email respondents were 471 (43.98%), email not using respondents were 98 (9.15%). It also shows that 471 (43.98%) of respondents were using both personal and office email in their daily life, and Personal & Office email is the highest percentage than other email categories respondents. The email utilization respondents' rate was higher than not using respondents because most of the respondents were graduates and employees. The Female respondents' email utilization was high because, in this survey, the female respondent population was higher than male respondents.

Table (4.5) Internet Banking Usage by Respondents' Gender Class

Internet Banking	Male	Female	Total
Used	290 (27.08%)	512 (47.80%)	802 (74.88%)
Not Using	91 (8.50%)	178 (16.62%)	269 (25.12%)

Source: Survey data, 2020

Table (4.5) described the percentage of internet banking utilization by respondents. In all total 1071 respondents, 290 (27.08%) male respondents were using

internet banking and 91 (8.50%) male respondents were not using internet banking. In the female respondents, a total 512 (47.80%) of female respondents were using internet banking and 178 (16.62%) were not using internet banking Total number of internet banking usage was 802 (74.88%), the total number of not using respondents were 269 (25.12%). The number of Internet banking users was the highest number than not utilized respondents. It was also found that some of the respondents were not using Internet banking because these respondents were not familiar with Internet banking applications and some respondents were lack of trust in internet banking platforms.

Table (4.6) Frequency of the Respondents Mostly Used Social Medias Sites

Type of Social Medias	Male	Female	Total
Facebook	371 (34.64%)	675 (63.03%)	1046 (97.67%)
Instagram	10 (0.93%)	15 (1.40%)	25 (2.33%)
Twitter	0	0	0
LinkedIn	0	0	0
Snap Chat	0	0	0
VK	0	0	0
Reddit	0	0	0

Source: Survey data, 2020

Table (4.6) described the frequency of social media sites that mostly used by respondents. To analyzed these mostly used social media sites, the question was constructed by 7 kinds of most prominent social media sites around the world, these are Facebook, Instagram, Twitter, LinkedIn, Snap Chat, VK, and Reddit. It was found that 371 (34.64%) male respondents were mostly used Facebook social media site and only 10 (0.93%) of male respondents were mostly used Instagram. 675 (63.03%) female respondents were mostly used Facebook and 15 (1.40%) female respondents were mostly used Instagram. The total number of respondents who mostly used Facebook was 1046 (97.67%) and Instagram users were 25 (2.33%). Other social media sites are rarely used by respondents. In this table, it was found that Facebook was the respondents' most using social media site and also a prominent site among the respondents. Among the respondents, Twitter, LinkedIn, Snap Chat, VK, and Reddit social media platforms were using very rare because these sites were not only unfamiliar and but also not as prominent as Facebook and Instagram.

Table (4.7) Number of Respondents' Most Knowing Cybercrimes Cases

Cybercrimes Cases	Male	Female	Total
Fraud	340 (31.75%)	613 (57.23%)	953 (88.98%)
Hacking	56 (5.23%)	27 (2.52%)	83 (7.75%)
Cyberbullying	10 (0.93%)	10 (0.93%)	20 (1.86%)
Cyber Harassment	2 (0.18%)	8 (0.75%)	10 (0.92%)
Virus	2 (0.18%)	3 (0.28%)	5 (0.46%)
Child Pornography	0 (0.00%)	0 (0.00%)	0 (0.00%)

Source: Survey data, 2020

Table (4.7) described the respondents' most knowing cybercrimes cases, 953 (88.98%) respondents, their most knowing cybercrimes case was Fraud. Total 83 (7.75%) respondents' most knowing cybercrimes case was Hacking. Respondents 20 (1.86%), their most knowing cybercrimes case was Cyberbullying. Total respondents 10 (0.92%) most knowing cybercrimes case was Cyber Harassment and 5(0.46%) respondents' most knowing case was Virus. Child pornography case was no respondents knowing on it. The Fraud case was the most known case by the respondents.

4.4 Analyzing Respondents' Cybercrimes Knowledge

The Internet offers more educational and economic opportunities than any other the world has ever seen. Through the dangerous use of technology, cybercriminals can destroy businesses and even lives. Many organizations around the world are striving to eliminate criminals and help increase system securities. However, the best ways of prevention are knowledge and actual practices.

To analyze the respondents' cybercrimes knowledge, it was constructed by 7 cybercrimes basics knowledge questions. If the respondent's answer was right on one question, this respondent will get 1 score marks. If the respondent answers were right in all seven questions the respondent will have 7 marks. To defined respondents' cybercrimes knowledge, the mean scale score was calculated in each cybercrimes basic question. To describe the knowledge levels there were categorized by three levels, these were Weak, Moderate, and Good levels in each question. The Weak level represented

the score marks 0.0 to 0.4, the Moderate level represented the score marks 0.5 to 0.6 and the Good level was 0.7 to 0.9 score marks.

Table (4.8) Respondents' Cybercrimes Knowledge Levels

Basic Cybercrimes Knowledge Questions	Yes		Total	Mean Score	Knowledge Levels
	Male	Female			
Do you know that a close relationship with a stranger on online is dangerous?	166 (15.50%)	327 (30.53%)	493 (46.03%)	0.5	Moderate
Do you think that your privacy & information are safe by using all in one password for all accounts?	157 (14.66%)	312 (29.13%)	469 (43.79%)	0.4	Weak
Do you know that Public Wi-Fi is not safe for online banking transition?	184 (17.18%)	336 (31.37%)	520 (48.55%)	0.5	Moderate
Do you know that sharing privacy & private information on social media and chat rooms is a risk to become cyber victims?	356 (33.24%)	623 (58.17%)	979 (91.41%)	0.9	Good
Do you know that password leaking can occur when you click the link that someone shares or sends online?	345 (32.21%)	626 (58.45%)	971 (90.66%)	0.9	Good
Do you know that using Crack & Patch software can be infected viruses, abuse your data and computer system damage as well?	187 (17.46%)	293 (27.36%)	480 (44.82%)	0.4	Weak
7. Are basic cybercrimes awareness trainings or campaigns very needed to avoid potential cybercrimes?	259 (24.18%)	459 (42.86%)	718 (67.04%)	0.7	Good

Source: Survey data, 2020

Table (4.8) described respondents' cybercrimes knowledge levels in each cybercrimes knowledge questions. The data were calculated based on a total of 1071 respondents. Regarding close relation with a stranger on the online question, in this question, it was found that 166 (15.50%) male respondents and 327 (30.53%) of female respondents have good knowledge. Total good knowledge respondents were 493 (46.03%). Analyzing by mean score scale on this question by 1071 respondents, it was found that the mean score scale was 0.5, and respondents' awareness levels were moderate level in this relation closely with a stranger on the online question.

Respondents' cybercrimes knowledge regarding the safeguarding of privacy and information by using all in one password for all accounts, the result found that 157 (14.66%) of male respondents and 312 (29.13%) of female respondents have good knowledge. Total respondents who have good knowledge in the safeguarding of privacy and information were 469 (43.79%) respondents. Analyzing by the mean score scale to determine respondents' knowledge levels it was found that the mean score scale was 0.4 and respondents' cybercrimes knowledge levels were weak in the safeguarding of privacy and information by using all in one password for all accounts question.

Cybercrimes knowledge question regarding making bank transition by using public Wi-Fi, it was found that 184 (17.18%) of male respondents and 336 (31.37%) of female respondents were good knowledge respondents. Total good knowledge respondents were 520 (48.55%). Analyzing by mean score scale on this question, the result found that the mean score scale was 0.5, and the respondents' knowledge levels were moderate.

Regarding sharing private information on social media and chat room question, in this question, the result found that 356 (33.24%) of male respondents and 623 (58.17%) of female respondents were good knowledge. Total good knowledge on this sharing private information on social media and chat room respondents were 979 (91.41%). To analyze the knowledge level of respondents, it was found that the mean score scale was 0.9 therefore the respondents' knowledge levels were good.

Respondents' knowledge regarding clicking the link online can occur password leaking question, in this question, 345 (32.21%) of male respondents and 626 (58.45%) of female respondents were good knowledge respondents and total good knowledge respondents were 971 (90.66%). By using the mean score scale to analyze the total respondents' knowledge on this question, the result found that the mean score scale was

0.9 so that the respondents' knowledge levels were good in this password leaking can occur through by clicking the link online that someone sends or shares.

The respondents' knowledge question that related with virus infection by using crack & patch software, the result found that 187 (17.46%) of male respondents and 293 (27.36%) of female respondents were good knowledge respondents. The total good knowledge respondents were 480 (44.82%) respondents. The mean score scale was used to determine the respondents' knowledge levels, it was found that the mean score scale was 0.4, therefore the respondents' knowledge levels on this question were weak level.

Respondent's knowledge on the need of cybercrimes awareness training or campaigns to avoid potential cybercrimes questions, the result found that 259 (24.18%) of male respondents and 459 (42.86%) of female respondents were good knowledge and total respondents who have good knowledge were 718 (67.04%). To describe the total respondents' knowledge levels, the mean score scale was using and it was found that the mean score scale was 0.7, therefore the respondents' knowledge levels were good and the respondents knew the need for cybercrimes awareness training or campaigns to avoid potential cybercrimes.

The overall finding regarding respondents' cybercrimes knowledge levels, it was found that the respondents were weak knowledge levels on the safeguarding of privacy and information because the respondents do not know the danger of all in one password for all of their accounts. Then the respondents were also weak in knowledge on using crack & patch software because the respondents did not know about a virus infection, abuse information that can happen through using crack & patch software. The respondents' knowledge levels were moderate levels in close relation with a stranger on online and making banking transition through public Wi-Fi questions. The respondents' knowledge levels were good in sharing private information on social media and chat room, password leaking can occur by clicking internet links and important of basic cybercrimes awareness & campaign to prevent potential cybercrimes.

4.4.1 Cybercrimes Knowledge Level of All Respondents

To describe the cybercrimes knowledge level of all respondents, the mean score scale was calculated by using the total marks of all respondents based on respondents' answers to all cybercrimes knowledge questions. To define the levels, it was used three

categories, which were Weak and Moderate, and Good levels. The Weak level represented the score marks 0 to 3, the Moderate level represented the score marks 4 to 5 and the Good level was 6 to 7 score marks.

Table (4.9) Cybercrimes Knowledge Level of All respondents

Mean Score	Weak (0-3)	Moderate (4-5)	Good (6-7)
4.3	-	Moderate Level	-

Source: Survey data, 2020

Table 4.9 described the cybercrimes knowledge level of all respondents, it was found that the total score marks of respondents in all cybercrimes knowledge questions was 4630.To define the respondents' knowledge levels on all of the cybercrimes knowledge questions the mean score scale was 4.3. Therefore cybercrimes knowledge level of all respondents was moderate levels.

4.4.2 Analyzing Respondents' Actual Practices

This is to study the respondents' actual practices while they are using the internet. Only knowledge is not enough to prevent cybercrimes, the other important thing that is still needed, it is actual practices. if a lack of good actual practices for safeguarding privacy, information, and data while using internet services it is very dangerous and as if welcomes to cybercrimes. The actual practice is very important to avoid cybercrimes problems and potential cybercrimes risks. In this actual practices questions were constructed by seven basic questions. Total 1071 respondents were responded with their internet services using practices.

To analyze the respondents' actual practices, it was constructed by 7 actual practices questions. If the respondent's answer was right on one question, this respondent will get 1 score marks. If the respondent answers were right in all seven questions the respondent will have 7 marks. To defined respondents' actual practices, the mean scale score was calculated in each question. To describe the actual practice levels there were categorized by 3 levels, these were Weak, Moderate, and Good levels in each question. The Weak level represented the score marks 0.0 to 0.4, the Moderate level represented the score marks 0.5 to 0.6 and the Good level was 0.7 to 0.9 score marks.

Table (4.10) Respondents' Actual Practices Levels

Actual Practices Question	Male	Female	Total	Mean Score	Knowledge Levels
	Yes	Yes	Yes		
1. Have you ever stay closely related to strangers on social media like your close friends?	187 (17.46%)	293 (27.36%)	480 (44.82%)	0.4	Weak
2. Do you use all in one password for all your account?	162 (15.13%)	280 (26.14%)	442 (41.27%)	0.4	Weak
3. Have you ever use public Wi-Fi for your banking transition?	176 (16.43%)	288 (26.89%)	464 (43.32%)	0.4	Weak
4. Do you used to share your privacy and information on social media and chatting room?	259 (24.18%)	459 (42.86%)	718 (67.04%)	0.7	Good
5. Have you ever click the link that shares or send on social media, email, and online?	260 (24.28%)	512 (47.81%)	772 (72.09%)	0.7	Good
6. Do you use Crack & Patch software at your business?	54 (5.04%)	118 (11.02%)	172 (16.06%)	0.2	Weak
7. Have you ever attended training or campaigns for cybercrimes awareness or other related cyber security?	77 (7.19%)	170 (15.87%)	247 (23.06%)	0.2	Weak

Source: Survey data, 2020

Table (4.10) described the respondents' actual practice levels. Regarding closely related with a stranger on the online question, 187 (17.46%) of male respondents and 293 (27.36%) have good practices. Total good practices respondents who do not relate closely with strangers on online were 480 (44.82%).To analyses the total respondents' actual practices levels, the mean score scale on this question was 0.4 therefore the respondents were weak actual practices.

Regarding all in one password using for all accounts, in this question, 162 (15.13%) of male respondents and 280 (26.14%) of female respondents were good actual practices. Total good actual practices respondents who do not use all in one password for all accounts were 442 (41.27%). Data analysis by the mean score scale

for all respondents, the result found that mean score scale was 0.4 so that the respondents' actual practices were weak in using all in one password for all account question.

The respondents' banking transition practices through public Wi-Fi question. In this question, 176 (16.43%) of male respondents and 288 (26.89%) of female respondents were good actual practices. Total good actual practices respondents were 464 (43.32%) respondents. Analyzing by using the mean score scale to describe all respondents' actual practices on banking transition using public Wi-Fi, it was found that the mean score scale was 0.4. The result was the respondents' actual practices were weak.

Respondent's actual practices for sharing their information on social media and chatrooms question, in this question, 259 (24.18%) of male respondents and 459 (42.86%) of female respondents were good actual practices. Total good respondents who don't share their private and privacy information were 718 (67.04%). Using the mean score scale to describe the level of all respondents' actual practices the mean score scale was 0.7. Therefore the respondents' actual practice level was good in regarding sharing private information online.

The respondents' actual practices for clicking the links from someone to share or send on the internet question. In this question, total male respondents 260 (24.28%) and 512 (47.81%) of female respondents were good actual practices. The total of respondents who good in actual practices was 772 (72.09%) respondents. The mean score scale result for all respondents regarding this question was 0.7. So that the respondents' actual practices were good practices.

Regarding the crack & patch software using respondents' practices in the business. In this question, it was found that 54 (5.04%) of male respondents and 118 (11.02%) of female respondents were good practices because they don't use crack & patch software in their business. Total respondents who good in actual practices were 172 (16.06%) respondents. The result of all respondents the mean score scale was 0.2. Therefore the respondents' actual practices level of using crack & patch software using on their business were weak practices.

Regarding respondents' cybercrime awareness training or campaigns, in this question, 77 (7.19%) of male respondents and 170 (15.87%) of female respondents have been attended cybercrimes awareness training or campaigns. The total number of respondents who had been attended related to cybercrimes awareness training or

campaigns was 247 (23.06%). To describe the actual practices level of total respondents, it was using the mean score scale, the mean score scale result was 0.2 so that the respondents' actual practices in cybercrime awareness training or related cybersecurity campaigns were weak.

The overall finding on respondents' actual practices levels, the respondents were weak practices on in relating with stranger like the close one on social media this means that these respondents do not consider the consequences of related cybercrimes by these strangers. Then it was also found that the respondents' actual practices were weak on using all in one password for all accounts this is very dangerous if they have leaked one of account's password then all of their accounts will the under the cybercriminal control the consequence of many cyberbullying, cyber harassment, fraud and other more cybercrimes case will be occur. Regarding banking transition over the public Wi-Fi, the respondents were weak practices because the respondents were used public Wi-Fi for banking transition. By using this public Wi-Fi for banking transition services, the cybercriminal can be seen easily data streaming on public Wi-Fi, which means the attacker can steal or change the data over the public Wi-Fi, as the consequences the fraud and other cybercrimes can occur. The result also found that respondents were weak practices in using crack & patch software in their business, the consequence of using crack & patch software, the confidential data, business data, and personal data can be stolen or abuse and virus infection can be faced on business. Regarding the cybersecurity and cybercrimes awareness training, it was also found that the respondents' actual practices were weak. The lack of training and campaigns the respondent cannot get the information about for safe internet use, prevention, and action for how to handle & report the cybercrimes.

In the respondents' actual practices question, the good result found that the respondents' actual practices levels were good in sharing privacy & private information on social media & chat room question and the respondents were also good practices levels on clicking online link that someone share or send. This mean that respondents were good practices and knowledge about the safeguarding of privacy and private information and password leaking.

4.4.3 Actual Practices Level of All Respondents

To describe the actual practices level of all respondents, the mean score scale was calculated by using the total marks of all respondents based on respondents'

answers to all actual practices questions. To define the levels of actual practices, it was used three categories, which were Weak and Moderate, and Good levels. The Weak level represented the score marks 0 to 3, the Moderate level represented the score marks 4 to 5 and the Good level was 6 to 7 score marks.

Table (4.11) Actual Practices Level of All respondents

Mean Score	Weak (0-3)	Moderate (4-5)	Good (6-7)
3.0	Weak Level	-	-

Source: Survey data, 2020

Table 4.11 described the actual practices level of all respondents, it was found that the total score marks of respondents in all actual practice questions was 3295.To define the respondents' actual practice levels on all of the actual practice questions ,the mean score scale was 3.0. Therefore actual practices level of all respondents was weak levels.

4.4.4 Analyzing Respondent's Cybercrimes Awareness levels

To measure cybercrimes awareness levels, firstly it is important for the respondents' knowledge on cybercrimes what they have known and what they don't know, and then their actual practices how they were using the internet safely. Therefore, to examine the cybercrimes awareness levels of Yangon internets users was constructed by two question types, these were knowledge and actual practice questions. To analyze the cybercrimes awareness levels the two question types were constructed these were the cybercrimes knowledge questions with 7 cybercrimes basic knowledge questions and actual practices questions of 7 practices questions. In each question total 1071 respondents were responded by their knowledge and practices.

In the cybercrime knowledge questions, the respondents have moderate levels in relation closely with a stranger on online but in the respondents' actual practices were weak. Regarding this close relation with strangers on online, knowledge, and practices questions, it was found that the respondents were weak in awareness level.

Regarding using all in one password knowledge and actual practices questions, it was found that the respondents were weak in both knowledge and actual practices. This means that respondents were using all in one password for all of their accounts. Therefore, the respondents' awareness levels were weak.

The respondents' awareness levels on using public Wi-Fi, it was found that the respondents' knowledge was moderate but the respondents' actual practices were weak. This means that the respondents don't know the danger of public Wi-Fi for banking transition therefore the respondents' awareness levels were weak.

Sharing privacy & private information on social media and chat rooms, the respondents were good in both cybercrimes knowledge and practices. It was found that the respondents were good awareness levels for the consequence danger of sharing privacy & private information on social media and chat rooms.

Respondents' awareness levels on password leaking can occur by clicking an internet link that someone shares or send, it was found that the respondents were good in both cybercrimes knowledge and practices. The respondents have good awareness levels because they know password leaking can occur by clicking the internet link.

Using Crack & Patch software in the business, it was found that the respondents were weak in both knowledge and practices, they do not know the consequence of potential cybercrimes through by crack & patch software, and therefore the respondents were weak cybercrimes awareness levels.

Regarding cybercrimes awareness or related cybersecurity training or campaigns, in this knowledge and practices question, it was found that the respondents were good in cybercrimes knowledge but weak in actual practices. The respondents have good knowledge of needed training and campaigns to prevent cybercrimes but their actual practices were weak therefore the respondents' cybercrimes awareness levels were weak.

The result for each knowledge and practice questions, the respondents were moderate and good levels in cybercrimes knowledge but generally weak in actual practices. Only good knowledge is not enough to prevent potential cybercrimes because the important thing is their actual practices while using online. The respondents should have a good level in both of cybercrimes knowledge and actual practices for using the internet services to avoid cybercrimes cases. The overall result that represented to all of respondents levels in knowledge and practices questions, it was found that the cybercrimes knowledge level of all respondents was moderate level and actual practices level of all respondents was weak levels. Therefore the result found that the respondents were weak in cybercrime awareness levels.

4.4.5 Respondents' Awareness on Myanmar's Cyber Laws

The law protects public safety and guarantees and rights for citizens to against abuse by others, by organizations, and by governments. This section was constructed by two questions to analyze respondent's awareness of Myanmar laws that can punish to cybercriminals and to examine the cybercrimes related laws that the respondents know.

Below Table. (4.12) showed that the result of the respondents' knowledge on enacted the law to punish cybercriminals in Myanmar. In this question yes, mean the respondents know the punishment law. No, this means that Myanmar has no enacted law to punish cybercriminals. Don't Know, means that don't know if have or not.

Table. (4.12) Respondent's Knowledge on Laws to Punish Cybercriminals

Particular	Yes	No	Don't Know
Knowledge on Cybercriminal Punishment law	483 (45.10%)	157 (14.66%)	431 (40.24%)

Source: Survey data, 2020

Regarding this question 483 (45.10%) respondents knew that there have cybercrimes-related laws and regulations to punish cybercriminals in Myanmar. 157 (14.66%) respondents were answered that there has no related laws and regulations to punish cybercriminals in Myanmar. 431 (40.24%) of respondents, did not know if Myanmar has the laws and regulations to punish cybercriminal law or not. The result found that the respondents' awareness was very weak regarding laws and regulations related to cybercrimes.

Table. (4.13) Enacted Cybercrimes Related Law That Respondents Known

Particular	Telecommunication Law (66D)	Electronic Transition Law	Don't Know
Respondents most knowing Cybercrimes Related law	290 (27.08%)	0	781 (72.92%)

Source: Survey data, 2020

Table. (4.13) described that the respondents the most noticed for cybercrimes related laws, 290 (27.08%) of respondents were knowing Telecommunication law

section (66D) and 781 (72.92%) respondents did not know the cybercrimes related laws. No one knows the Electronic Transition law among the respondents. The result was Telecommunication Law (66D) was the prominent law and the respondents were weak knowledge on related cybercrimes law.

4.5 Analyzing Respondents' Cybercrimes Experiences

The respondents' experiences section, this section was aimed to analyze the cybercrimes cases used to happen among Yangon internet users. This experiences section was constructed by 13 cybercrimes experiences questions these questions were constructed by cybercrimes cases and contents because if the questions were direct mention in cybercrime types (e.g., Fraud, Ransomware. etc.) the respondents might not understand and difficult to decide based on their experiences. In each question was structured into four categories, these are experienced by myself, friends, media, no experiences.

Below table (4.14) described that frequency and percentage of the respondents' cybercrimes experiences by cybercrimes types. In this table, 323 (30.16%) of male respondents experienced fraud cases and 616 (57.52%) of female respondents also had experiences with fraud cases. Total experiences of fraud case who have experienced were 939 (87.67%) respondents. In this fraud case, there have 58 (5.41%) of male respondents have never experiences and 74 (6.91%) of female respondents have no experience in fraud cases. The number of no experiences on fraud case respondents were 132 (12.32%).

Regarding cyberbullying cases, there have 261 (24.37%) of male respondents have cyberbullying experiences, and 569 (53.13%) of female respondents have experiences with cyberbullying. The total number of respondents' experiences with cyberbullying was 830 (77.50%).120 (11.20%) of male respondents were no experiences and 121 (11.30%) of female respondents have also no experiences with cyberbullying. The total number of respondents no experience cyberbullying respondents was 241 (22.50%).

The respondents' experiences on cyber harassment, 255 (23.81%) of male respondents, and 570 (53.22%) of female respondents have cyber harassment experiences. The total number of respondents who have experience in cyber harassment was 825 (77.03%) respondents. 126 (11.76%) of male respondents and 120 (11.20%)

female respondents were no experience with cyber harassment. Total no experiences on cyber harassment respondents were 246 (22.97%).

Table (4.14) Respondents' Cybercrimes Experiences by Types

Cybercrime Types	Cybercrimes Experience			Cybercrimes No Experience		
	Male	Female	Total	Male	Female	Total
Fraud	323 (30.16%)	616 (57.52%)	939 (87.67%)	58 (5.41%)	74 (6.91%)	132 (12.32%)
Cyberbullying	261 (24.37%)	569 (53.13%)	830 (77.50%)	120 (11.20%)	121 (11.30%)	241 (22.50%)
Cyber harassment	255 (23.81%)	570 (53.22%)	825 (77.03%)	126 (11.76%)	120 (11.20%)	246 (22.97%)
Hacking	267 (24.93%)	542 (50.61%)	809 (75.54%)	114 (10.64%)	148 (13.82%)	262 (24.46%)
Spamming	269 (25.12%)	521 (48.65%)	790 (73.76%)	112 (10.46%)	169 (15.78%)	281 (26.24%)
Virus	271 (25.30%)	506 (47.24%)	777 (72.55%)	110 (10.27%)	184 (17.18%)	294 (27.45%)
Scamming	259 (24.18%)	502 (46.87%)	761 (71.05%)	122 (11.39%)	188 (17.55%)	310 (28.94%)
Identify theft	255 (23.81%)	487 (45.47%)	742 (69.28%)	126 (11.76%)	203 (18.95%)	329 (30.72%)
Social engineering	244 (22.78%)	461 (43.04%)	705 (65.83%)	137 (12.79%)	229 (21.38%)	366 (34.17%)
Child pornography	201 (18.77%)	448 (41.83%)	649 (60.60%)	180 (16.81%)	242 (22.59%)	422 (39.40%)
Malvertising	212 (19.79%)	420 (39.21%)	632 (59.01%)	169 (15.78%)	270 (25.21%)	439 (40.99%)
Phishing	201 (18.77%)	383 (36.76%)	584 (54.53%)	180 (16.81%)	307 (28.66%)	487 (45.47%)
Ransomware	211 (19.70%)	359 (33.52%)	570 (53.22%)	170 (15.87%)	331 (30.91%)	501 (46.78%)

Source: Survey data, 2020

Respondents' experiences of hacking were 267 (24.93%) of male respondents and 542 (50.61%) were female respondents. The total number of respondents who have experience in hacking was 809 (75.54%) respondents. 114 (10.64%) of male

respondents and 148 (13.82%) female respondents were no experience in hacking. Total 262 (24.46%) respondents were no experiences in hacking.

Regarding respondent's experiences with Spamming, in this cybercrime case, 269 (25.12%) of male respondents and 521 (48.65%) of female respondents have experiences with spamming. Total 790 (73.76%) respondents have experiences with spamming.122 (11.39%) of male respondents and 169 (15.78%) of female respondents have no experiences with spamming. Total no experiences with spamming respondents were 281 (26.24%).

Respondents' experiences on the virus, it was found that 271 (25.30%) of male respondents and 506 (47.24%) of female respondents have experiences on virus infection on their devices. The total number of respondents' experiences with the virus was 777 (72.55%).110 (10.27%) of male respondents and 184 (17.18%) of female respondents were no experience in virus infection on their devices. Total no experiences on virus respondents were 294 (27.45%).

The respondents' experiences Scamming, 259 (24.18%) of male respondents and 502 (46.87%) of female respondents have experienced. The total respondents who have experiences in scamming cases were 761 (71.05%).122 (11.39%) of male and 169 (15.78%) of female were the respondents who never have scamming experiences. The total number of no experiences respondents were 310 (28.94%).

Regarding identify theft respondents' experiences, there were 255 (23.81%) of male respondents and 487 (45.47%) of female respondents who have experiences on identify theft. Total respondents' experiences on identify theft were 742 (69.28%).126 (11.76%) of male respondents and 203 (18.95%) of female respondents were no experiences of identify theft. The total number of respondents who don't have experiences was 329 (30.72%).

The respondents' experiences on social engineering, it was found that there were 244 (22.78%) of male respondents and 461 (43.04%) of female respondents have experiences in social engineering. The total number of respondents who have experienced were 705 (65.83%) respondents. 137 (12.79%) of male respondents and 229 (21.38%) of female respondents were no experiences in social engineering. The total number of no experiences respondents were 366 (34.17%).

The result found that on child pornography experiences, there have 201 (18.77%) of male respondents and 448 (41.83%) of female respondents experienced child pornography. The total number of respondents who have experienced was 649

(60.60%). 180 (16.81%) of male respondents and 242 (22.59%) of female respondents were never have child pornography experiences. Total 422 (39.40%) respondents were no experiences with child pornography.

The respondents' experiences on malvertising, the result found that 212 (19.79%) of male respondents and 420 (39.21%) of female respondents were who have experiences of it. The total number of respondents who have experience in malvertising was 632 (59.01%). 169 (15.78%) of male respondents and 270 (25.21%) female respondents were no experiences of malvertising. The total number of no experiences respondents were 439 (40.99%).

Regarding respondents' phishing experiences, there were 201 (18.77%) male respondents and 383 (36.76%) female respondents who have experiences with phishing. The total number of respondents who have experiences on phishing was 584 (54.53%).180 (16.81%) of male and 307 (28.66%) of female respondents were never seen a phishing attack. The total number of no experiences respondents was 487 (45.47%).

Respondents' experiences on Ransomware, the result found that 211 (19.70%) of male respondents and 359 (33.52%) female respondents were who have experiences in Ransomware. Total respondents' experiences with ransomware were 570 (53.22%). 170 (15.87%) of male respondents and 331 (30.91%) of female respondents were no experiences with ransomware. The total number of respondents who never have experiences with ransomware was 501 (46.78%).

Overall result on cybercrimes experienced by respondents, in all of cybercrimes cases, the fraud cases was the highest number of respondents' experiences because the respondents were weak in cybercrimes knowledge & practices while using online banking transition such as mobile banking, internet banking, wave money, and many other online money transition platforms and the respondents were weak in password security for respective services. The second highest cybercrimes respondents' experiences were cyberbullying cases and the third one was cyber harassment cases, because the respondents were widely used social media platforms & online chatting rooms with weak cybercrimes awareness levels especially relation closely with a stranger on online, safeguarding for privacy and information. Therefore the consequence effects were rising cyberbullying and cyber harassment cases. The other remains cybercrimes cases theses were needed for complicated technical skills and the attacker need high tech therefore, the respondents' experiences were low.

4.5.1 Analyzing Respondents' Experiences and Information Sources

Respondents' cybercrimes experiences and information sources, the respondents were responded base on their experiences and information for respective cybercrimes cases that they faced. Depending on the respondents' experiences, the result of cybercrimes experiences and information sources were not constant. Regarding the experiences and information, some respondents have experienced by themselves only and some have experienced only from their friends and some have information only from Medias. Some respondents have experiences and information from more than one source (example from Self-experiences and experiences by their friends) and some respondents have from all sources (Self, Friends, Media).

Below Table (4.15) described regarding fraud, the total number of self-experiences was 83 (7.75%), the total number of experiences form respondents' friends were 220 (20.54%), the total number of information form Medias respondents were 330 (30.81%), the total number of information and experiences from two sources respondents were 268 (25.02%) and the total number of experience and information from all sources respondents were 38 (3.55%).

The result of respondents' experiences and information sources for cyberbullying, the total number of self-experience respondents were 124 (11.58%), the total number of respondent friends' experiences were 131 (12.23%), total cybercrimes information form the medias respondents were 383 (35.76%), the number of respondents who have experiences and information form the two sources were 162 (15.13%) and experiences and information from all sources respondents were 30 (2.80%).

The respondents' experiences and information result for cyber harassment, total self-experiences respondents were 257 (24.00%), total number respondent friend's experiences were 129 (12.04%) respondents and information from the media total respondents were 248 (23.15%), the respondents who have from two sources were 191 (17.83%) and there have no respondents who have experiences and information for all sources.

Regarding the respondents' experiences on hacking, the number of self-experiences respondents was 47 (4.39%), the number of respondent friends' experiences on hacking was 167 (15.59%), information form Medias respondents were 369 (34.45%), the number of two sources respondents were 188 (17.55%) and 38 (3.55%) respondents have experiences and information for all sources.

Table (4.15) Information Sources of Respondents' Cybercrimes Experiences

Cybercrime Types	Sources of Experiences and information				
	One Source			Two Sources	All Sources
	Self	Friends	Medias		
Financial Fraud	83 (7.75%)	220 (20.54%)	330 (30.81%)	268 (25.02%)	38 (3.55%)
Cyberbullying	124 (11.58%)	131 (12.23%)	383 (35.76%)	162 (15.13%)	30 (2.80%)
Cyber harassment	257 (24.00%)	129 (12.04%)	248 (23.15%)	191 (17.83%)	0 (0.00%)
Hacking	47 (4.39%)	167 (15.59%)	369 (34.45%)	188 (17.55%)	38 (3.55%)
Spamming	483 (45.10%)	43 (4.01%)	68 (6.35%)	99 (9.24%)	97 (9.06%)
Virus	396 (36.97%)	78 (7.28%)	68 (6.35%)	122 (11.39%)	113 (10.55%)
Scamming	414 (38.65%)	65 (6.07%)	76 (7.10%)	124 (11.58%)	82 (7.65%)
Identify theft	60 (5.60%)	190 (17.74%)	229 (21.38%)	235 (21.94%)	28 (2.61%)
Social engineering	236 (22.03%)	113 (10.55%)	140 (13.07%)	146 (13.63%)	70 (6.53%)
Child pornography	80 (7.47%)	68 (6.35%)	421 (39.31%)	60 (5.60%)	20 (1.87%)
Malvertising	438 (40.90%)	51 (4.76%)	0 (0.00%)	0 (0.00%)	143 (13.35%)
Phishing	49 (4.57%)	103 (9.62%)	321 (29.97%)	101 (9.43%)	10 (0.93%)
Ransomware	268 (25.02%)	53 (4.95%)	89 (8.31%)	87 (8.12%)	73 (6.82%)

Source: Survey data, 2020

The result for the spamming attack experiences, there have respondents self-experiences on spamming attacks were 483 (45.10%), respondents friends' experiences were 43 (4.01%), information from the medias respondents were 68 (6.35%), experiences and information for two sources respondents were 99 (9.24%) and

respondents who have experiences and information for all sources respondents were 97 (9.06%).

The result for respondents' experiences on the virus, there have 396 (36.97%) respondents have self-experience, 78 (7.28%) respondents have virus experiences on their friends, 68 (6.35%) respondents have information form media, 122 (11.39%) respondents have information and experiences form two sources and 113 (10.55%) respondents have information and experiences for all sources.

According to the result for the respondents' experiences on scamming attack, the respondents who have their own experiences were 414 (38.65%) respondents, 65 (6.07%) respondents' friends have spamming experiences, 76 (7.10%) respondents who have information for media, 124 (11.58%) respondents have experiences and information from two sources and 82 (7.65%) respondents have experiences and information from all sources.

Regarding identify theft, the total number of self-experiences were 60 (5.60%), the total number of experiences form respondent's friends were 190 (17.74%), the total number of information form medias respondents were 229 (21.38%), the total number of information and experiences from two sources respondents were 235 (21.94%) and the total number of experience and information from all sources respondents were 28 (2.61%).

As the result of social engineering experiences and information sources, the total number of self-experience respondents were 236 (22.03%), the total number of respondents friend's experiences were 113 (10.55%), total Social engineering information form the medias respondents were 140 (13.07%), experiences and information form the two sources number of respondents were 146 (13.63%) and experience and information from all sources respondents were 70 (6.53%).

The result for respondents' experiences on child pornography, there have 80 (7.47%) respondents has self-experience, 68 (6.35%) respondents have child pornography experiences on their friends, 421 (39.31%) respondents have information form media, 60 (5.60%) respondents have information and experiences form two sources and 20 (1.87%) respondents have information and experiences for all sources.

Regarding the respondents' experiences on malvertising, the number of self-experiences respondents was 438 (40.90%) respondents, the number of respondent friend's experiences on malvertising was 51 (4.76%), there have no respondents who

have information form Medias and no two sources respondents and 143 (13.35%) respondents who have experiences and information for all sources.

According to the study result for the respondents' experiences on phishing attack, the respondents who have their own experiences were 49 (4.57%) respondents, 103 (9.62%) respondents friends have phishing experiences, 321 (29.97%) respondents who have information for Medias, 101 (9.43%) respondents have experiences and information from two sources and 10 (0.93%) respondents have experiences and information from all sources.

The respondents' experiences and information result for ransomware, total self-experiences respondents were 268 (25.02%), total number respondents friend's experiences were 53 (4.95%) respondents and information from the medias total respondents were 89 (8.31%), the respondents who have from two sources were 87 (8.12%) and the number of respondents who have experiences and information for all sources was 73 (6.82%).

4.5.2 Analyzing Types of Cybercrimes Cases Used to Happen in Yangon

Every cyber-attacks have impacts on all victims, some cases impact on mental, some are impacted on the economy and some impact on socials and some have lost their lives by cybercrimes. The cybercrime impacts were different depending on cybercrime cases. At all of the cybercrimes experience questions, a total of 1071 respondents were responded with their experiences. The results were different depends on the respondents' experiences. Some respondents have their own, their friends, and also some have seen on media. Some respondents have no experiences. In these 1071 respondents, female respondents were 690 (64.43%) and male respondents were 381 (35.37%). The data calculation was computed based on a total of 1071 respondent's experiences. Table (4.12) was the result of the cybercrimes cases that the most happen among Yangon internet users, see below;

Table (4.16) Top Three Highest Cybercrimes Cases

Cybercrime Types	Cybercrimes Experiences By Gender		
	Male	Female	Total
Financial Fraud	323 (30.16%)	616 (57.52%)	939 (87.67%)
Cyberbullying	261 (24.37%)	569 (53.13%)	830 (77.50%)
Cyber harassment	255 (23.81%)	570 (53.22%)	825 (77.03%)

Source: Survey data, 2020

Table (4.16) described the top three highest cybercrimes cases that most happened among the respondents. The top three cybercrimes cases were (1) Financial Fraud, (2) Cyberbullying and (3) Cyber Harassment. Regarding the online fraud cases, 323 (30.16%) of male respondents have experiences and 616 (57.52%) of female respondents have experienced. In total out of 1071 respondents, the total of male and female respondent's online fraud experiences were 939 (87.67%).

In the cyberbullying case, a total of 261 (24.37%) male respondents have cyberbullying experiences, and 569 (53.13%) female respondents have cyberbullying experiences. Total male and female experiences on cyberbullying experiences were 830 (77.50%).

In the cyber-harassment cases, 255 (23.81%) of male respondents have experienced and the number of female respondents 570 (53.22%) have experienced cyber harassment. Total male and female experiences on cyber harassment experiences were 825 (77.03%).

Regarding the respondents' actions who have suffered cybercrimes, they handled themselves without reporting police because if they reported to the police they have to go police station and wasting their time at the police station and courts. Then lack of taking action on cybercrimes, therefore, the cyber victims were not reporting to the respective department. Most of the respondents don't know how to report cybercrimes to the police.

According to Table (4.16), the survey result showed that the respondents' experiences of online fraud cases were the highest respondents' experiences than other cybercrimes cases. Then the second highest cybercrime case was cyberbullying and the third one is cyber harassment cases. In these top three cybercrimes cases, the female

respondents were prone to cybercrimes than male respondents. According to the finding result of the cybercrimes crimes cases used to happen in Yangon was fraud cases.

The respondents' cybercrimes experiences were high because the cybercrimes knowledge level of all respondents was moderate level and the actual practice level of all respondents was weak levels. The respondents should have a good level in both of cybercrimes knowledge and actual practices for using the internet services to avoid cybercrimes cases. Therefore the respondents' cybercrimes awareness levels were weak. The consequences of weak level in cybercrimes awareness, the respondents did not know safe using of internet banking services, password security for respective services, the dark side of social media & chatting rooms and safeguarding of privacy & information. Therefore the result of cybercrimes experiences among the respondents was high.

CHAPTER V
CONCLUSION

5.1 Findings

ICT has become an important part of business running, organizations, education, E-banking, E-government, E-commerce, and also individual life. In this modern era, people have heavily relied on computer-related systems and internet services. With the development of ICT and Cyberspace, cybercrimes cases were rising around the globe. According to the historical record, the first cybercrime was committed as a phone phreak. With the development of technology, the cybercriminals were trying to develop cyber attacking techniques to meet with modern technology. The cybercriminals were targeted important data, information to get the benefit.

In Myanmar, before 2012 the cybercrime cases were very rare cases because at that time Myanmar had lagged behind in internet services and telecommunication services. After reforming of Telecommunication sectors Myanmar people have good internet services and telecommunication services, even the people who live in a remote area can access internet services. With the development of the internet and telecommunication services across the country in Myanmar, cybercrimes emerged. Before reforming to ICT sectors, Myanmar enacted just only two laws these two laws were Computer Science Development Law (1996) and Electronic Transaction Law (2004). After reforming the ICT sectors in Myanmar the new law Telecommunications Law (2013) was enacted to take action on cybercrimes-related cases. According to Cyber Police Department data, in 2019 the most reported cybercrimes cases were Fraud and Online Sexual cases (cyber harassment).

The primary objective of the survey is to examine the levels of cybercrime awareness of Internet users in Yangon and to identify the type of cybercrime cases that used to happen in Yangon. Structured questionnaires were used to collect all relevant information regarding cybercrimes knowledge, practices, and cybercrime experiences.

It was found that the number of total respondents was 1071. In total 1071 respondents, female respondents were 690 (64.43%) and male respondents were 381 (35.57%). By analytical with educational classes, for the female respondents, there are 592 (55.28%) graduate respondents, 95 (8.87%) female respondents were university level, 3 (0.28%) were high school levels and there had no primary school level respondents in female respondents. At the male respondents, 301 (28.10%) were graduate, 59 (5.51%) were university level, 13 (1.21%) were high school and 8 (0.75%) male respondents were primary level. In terms of educational classes, there are 893 (83.38%) Graduate respondents, 154 (14.38%) people were University level, 16 (1.49%) persons were High School levels, and 8 (0.75%) respondents in Primary School. The graduate level respondents were the highest number in total respondents. The highest rate of respondents' occupation was employee, 742 (69.28%) were employee and email type that the most respondents using type was Personal & Office Email. The most daily internet using time was 1 to 5 hours among the respondents and Facebook was the most used social media site among the respondents.

Regarding Rules and regulations related to cybercrimes, only 483 (45.10%) respondents knew that there has a regulation to punish cybercriminals in Myanmar. 157 (14.66%) respondents were answered that there has no related law to punish cyber-criminals in Myanmar. 431 (40.24%) of respondents, did not know if Myanmar has the law to punish cybercriminal law or not. The most prominent law was the Telecommunication law (66D), a total of 290 (27.08%) respondents were knowing of this law. The main finding of respondents' awareness in Law that related with cybercrimes section, the respondents' awareness were very weak on rules and regulations. And then law enforcement was also weak because of not enough respective technicians and the currently enacted laws were not fully cover all of the cybercrime cases especially data protection, child online protection, and critical infrastructure protection. It was also found that a lack of specific guidelines and procedures for respective departments and the international standard cyber laws is much needed to take action on cybercrimes cases in Myanmar.

Analyzing respondents' cybercrimes awareness levels the main finding were regarding closely relation with a stranger online, respondents were moderate level in cybercrimes knowledge but weak in actual practices, so that the result of respondents' cybercrimes awareness levels were weak. The respondents were closely related to the stranger online, which means that they don't know the danger of the consequences of

staying close with a stranger online. By staying closely with a stranger online, it can become stealing information, cyberbullying, cyber harassment, account hacking, and fraud, and many other crimes cases.

Using all in one password for all accounts question, the respondents were weak in both cybercrimes knowledge and practices questions, therefore, the respondents' cybercrimes awareness levels were weak because respondents were using all in one password for all their accounts, if the attacker knows just one account password then all accounts will be gone. This is very dangerous for safeguarding information and privacy.

The respondents' awareness levels on using public Wi-Fi, it was found that the respondents' knowledge levels were moderate and the respondents' actual practices were weak. This means that the respondents don't know the danger of public Wi-Fi for banking transition therefore the respondents' awareness levels were weak. Using banks transition over the public Wi-Fi respondents were using public, it is very dangerous to be stealing money from the network such as (fraud) because public Wi-Fi does not have good security (weak encryption) and the hacker can be snipping easily to change the data that streaming on public Wi-Fi.

Sharing privacy & private information on social media and chat rooms, the respondents were good in both cybercrimes knowledge and practices. It was found that the respondents were good awareness levels for the consequence danger of sharing privacy & private information on social media and chat rooms. Respondents' awareness levels on password leaking can occur by clicking an internet link that someone shares or send, it was found that the respondents were good in both cybercrimes knowledge and practices. The respondents have good awareness levels because they know password leaking can occur by clicking the internet link.

Respondents' awareness levels for using Crack & Patch software in the business, it was found that the respondents were weak in both knowledge and practices, they do not know the consequence of potential cybercrimes through by crack & patch software, and therefore the respondents were weak cybercrimes awareness levels. Using crack and patch software in the business, the business can be attacked by viruses, stealing sensitive data & confidential information then other many kinds of potential cyber-attacks can be faced through using these Crack / Patch software.

Regarding cybercrimes awareness or related cybersecurity training or campaigns, in this knowledge and practices question, it was found that the respondents

were good in cybercrimes knowledge but weak in actual practices. The respondents have good knowledge of needed training and campaigns to prevent cybercrimes but their actual practices were weak therefore the respondents' cybercrimes awareness level was weak. Without the cybercrimes awareness and campaigns the respondents don't know how to prevent cyber-attacks and what would they do they became cyber victims. The consequences of lacking cybercrimes awareness training and campaigns the cybercrimes rates can be high more and more.

The finding for cybercrimes experiences by respondents, it was found that the most used to the happened case was fraud cases, in this online fraud cases total 323 (30.16%) of male respondents have experienced and 616 (57.52%) of female respondents have experiences. Regarding the cyberbullying case, a total of 261 (24.37%) male respondents have cyberbullying experiences, and 569 (53.13%) female respondents have cyberbullying experiences. In the cyber-harassment cases, 255 (23.81%) of male respondents have experience and the number of female respondents 570 (53.22%) have experienced cyber harassment. According to the survey finding the result, which found that female respondents were prone to cybercrimes experiences than male respondents.

The overall finding of this study to examining awareness level and types of cybercrimes case used to happen among the Yangon internet users, especially graduate respondents were the highest 893 (83.38%) rate in this study. Although almost all of the respondents were graduate levels the finding result was the respondents' cybercrimes awareness levels were weak. Regarding the cybercrimes experiences, the female respondents have more experiences than male respondents. The online fraud cases were the most used to happen cybercrimes cases among the Yangon Internets users.

5.2 Suggestions

While the internet and the internet world are probably the best things that have ever happened to people, these new things also create a lot of problems and distractions in human daily life, it is called cybercrimes. To prevent cybercrimes the people should have awareness of cybercrime. In order to increase the cybercrime awareness level among the community, the main role is Government involvement and laws enforcement is very important. Then INGOs, NGOs, and media support to distribute cybercrimes knowledge to the community.

Regarding Rule and Regulations, Myanmar is still trying to enact cyber laws to meet the international standards to take action on cybercrimes cases. Now in Myanmar, there have three enacted laws that to take action for related to ICT and cybercrimes cases, these enacted laws were Computer Science Development Law (1996), Electronic Transaction Law (2004), and Telecommunications Law (2013). These laws were not full coverage of all cybercrimes cases such as data protection, child online protection, and critical infrastructure protection, etc. Therefore Myanmar should have complete international standard cyber law to protect the citizens and ICT infrastructure. To investigate cybercrimes, the respective departments should have more technicians, related updated software & hardware, and related ICT up to date devices. Then should have better collaboration and coordination with respective telecoms companies to tract out the cybercriminals. The government should promote cyber law to get more community awareness and the government should provide active hotline call centers, counseling and education centers.

Digital literacy skill is very important in the modern age. In Myanmar, schools do not teach regarding cyber advantage and disadvantage, at least children should know about cybercrimes as a basic in order to understand the importance of cybercrimes and how to protect themselves from potential cyber-attacks. If Government supports the digital skills curricula regarding the cyber advantages and disadvantages in the school education curricula it is a great idea to start growing the cybercrimes awareness skill for the generation. Therefore, the educational institution in Myanmar should have the active curriculum for cyber awareness among the students in order to increase their knowledge of cybercrimes and how to protect themselves from potential cyberattacks. For the peoples who have no opportunity to learn about cyber awareness in the school, it is grateful if the Government provides cybercrimes awareness training or campaigns, broadcasting cyber education movie on TV & Medias, and promote the cybercrimes laws & campaigns by collaborating with NGOs, INGOs to spread out cybercrimes knowledge around the whole country. At the cybercrimes awareness training or campaigns, it should be well planned sections such as rule & regulation, punishment by laws, what is the hotline contact number and address (Phone number, Email). Then the prevention section, consequences of cybercrimes and counselling for cyber victims. The cybercrimes awareness training or campaigns should be easy to access and attend for all people from all layers. Therefore the cybercrimes awareness levels would be high and people will know how to prevent and how to report the cybercrimes cases.

REFERENCES

Avais, M. A., Wassan, A. A., Narejo,H.,& Khan, J.A. (2014). Awareness Regarding Cyber Victimization Among Students of University of Sindh, Jamshoro. *International Journal of Asian Social Science*, 4 (5), 632-641. Retrieved from http://www.aessweb.com/pdf-files/ijass-2014-4 (5)-632-641.pdf

ASEANAPOL. (n.d.). *Myanmar Police Force*. Retrieved January 6, 2021, from http://www.aseanapol.org/information/myanmar-police-force

Achard, D. (n.d). *Cybercrime Situation.* Council of Europe. Retrieved from https://rm.coe.int/03-myanmar-presentation/168072bd20

Bussell, J. (2013, March 12). *Cyberspace Communications*. Britannica. Retrieved from https://www.britannica.com/topic/cyberspace

Casey, E. (2004). *Digital evidence and computer crime: Forensic science, computers, and the Internet* [2nd ed.]. Amsterdam: Academic Press.

Datareportal, (2020, February 18). *Digital 2020: Myanmar*. Datareportal. Retrieved from https://datareportal.com/reports/digital-2020-myanmar?rq=Myanmar%202020

Loader, B.D., & Thomas, D. (2000). Cybercrime: Security and Surveillance in the Information Age (1st ed.). Routledge. Retrieved from https://doi.org/10.4324/9780203354643

Daniels, J. (2017, November 29). IT Laws and Regulations in Myanmar: 5 Key Points to Consider. Lexology. Retrieved from https://www.lexology.com/library/detail.aspx?g=822a87b9-9a96-4627-8ed7-d8849644f849

Duverge, G. (2015, July 15). *Digital Threats: The Impact of Cyberbullying*. Touro University Worldwide. Retrieved from https://www.tuw.edu/health/impact-of-cyberbullying/

Desai, R. (2020, February 18). CYBERCRIME. Dr Rajiv Desai , An Educational Blog. Retrieved from https://drrajivdesaimd.com/2020/02/18/cybercrime/comment-page-2/

Erin, M. (2016, August 31). *A Personal History of the Internet in Myanmar*. The Henry M. Jackson School of International Studies Home. Retrieved from https://jsis.washington.edu/news/personal-history-internet-myanmar/

Ganti, A. (2020, April 29). *Rational Choice Theory*. Retrieved from Investopedia: https://www.investopedia.com/terms/r/rational-choice-theory.asp

Hernandez, E. (2018, February 14). *The 16 Most Common Types of Cybercrime Acts*. VoIP Shield (Utmost Defense Against CyberAttack). Retrieved from https://www.voipshield.com/the-16-most-common-types-of-cybercrime-acts/

James, K. (2019, May 9). *Digital development on steroids: Myanmar's rapid entry into the Internet era brings challenges as digital literacy lags*. DW Akademie: Retrieved from https://www.dw.com/en/digital-development-on-steroidsmyanmars-rapid-entry-into-the-internet-era-brings-challenges-as-digitalliteracy-lags/a-48669893

Khan, S. I. (2019, June 26). *The Paradox Of Cyber Crimes In Pakistan (part I)*. Daily Times. Retrieved from https://dailytimes.com.pk/418509/the-paradoxof-cyber-crimes-in-pakistan-part-i/

Knapton, S. (2018, Apirl 22). *Cyberbullying makes young people twice as likely to self harm or attempt suicide.* Telegraph. Retrieved from https://www.telegraph.co.uk/science/2018/04/22/cyberbullying-makes-youngpeople-twice-likely-self-harm-attempt/

Kumar, K.M., & Rajan, A. (2018). A Critical Study on Stalking and its Impact on Vulnerable Group of Women and Minors. *International Journal of Pure and Applied Mathematics*, 1709. Retrieved from https://acadpubl.eu/hub/2018-119-17/2/138.pdf

Kumar, K.M., & Rajan, A. (2018). A Critical Study on Stalking and its Impact on Vulnerable Group of Women and Minors. *International Journal of Pure and*

Applied Mathematics, 1710. Retrieved from https://acadpubl.eu/hub/2018-119-17/2/138.pdf

King Andrew. (2019, July 1). *Digital Literacy Training for Yangon Teachers.* Myanmar Times. Retrieved from https://www.mmtimes.com/news/digital-literacy-training-yangon-teachers.html

Lewis, J. (2018). *Economic Impact of Cybercrime-No Slowing Down.* Washington, D.C: Center for Strategic and International Studies. Retrieved from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Lee, H., & Lim H. (2019). Awareness and Perception of Cybercrimes and Cybercriminals. *International Journal of Cybersecurity Intelligence and Cybercrime*, 2 (1), 1-3. Retrieved from https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1018&context=ijcic

luyali. (2011, October 11). *The legal concept of cybercrime in Kenya*. Kenyaplex. Retrieved from https://www.kenyaplex.com/resources/2092-the-legal-concept-of-cyber-crimein-kenya.aspx

Mujovic', V. (2018, October 18). *Where Does Cybercrime Come From? The Origin & Evolution of Cybercrimes*. Le VPN. Retrieved from https://www.le-vpn.com/history-cyber-crime-origin-evolution/

MacKenzie, R., McEwan, T., Pathé, M., James, D., & Mullen, J. O. (2011). *Impact of stalking on victims*. Stalking Risk Profile. Retrieved from https://www.stalkingriskprofile.com/victim-support/impact-of-stalking-on-victims

Myanmar Law Information System. (n.d.).The computer science development law (1996). Retrieved from https://www.mlis.gov.mm/mLsView.do;jsessionid=FBF57F59FC7 4FC29B7FC08 9642B27DE6?lawordSn=26

Myanmar Law Information System. (n.d.).The electronic transactions law (2004). Retrieved from https://www.mlis.gov.mm/mLsView.do;jsessionid=7D02C63 E2E64C281E6E6 AC6CA1445665?lawordSn=1098

Myanmar Law Information System. (n.d.).The telecommunications law (2013). Retrieved from https://www.mlis.gov.mm/mLsView.do;jsessionid=92356 6A68C059E9E9 41BE 5045835F909?lawordSn=1076

mmCERT. (2020). Official website of the Myanmar Computer Emergency Response Team.mmcert.org.mm. Retrieved from https://www.mmcert.org.mm/about-us.html

Nam, K.Y., Cham, M. R., & Halili, P. R. (2015, November). *). Developing Myanmar's Information and Communication Technology Sector toward Inclusive Growth* (No. 462). Asian Development Bank. Retrieved from https://www.adb.org/sites/default/files/publication/176518/ewp-462.pdf

Nuccitelli, M (2011, November). *Cyber Harassment*. Ipredator. Retrieved from https://www.ipredator.co /cyber-harassment/

Naon, R., Schiffman, D., & Frank, F. (2018, March 28). *Cybercrime: a new threat in Myanmar*. CCI France Myanmar. Retrieved from https://ccifrance-myanmar.org/fr/event/cybercrime-anew-threat-in-myanmar

Ooredoo Myanmar. (2019, October 13). *Ooredoo becomes the first operator in Myanmar to collaborate with Google for a digital literacy and citizenship training program*. Ooredoo Myanmar. Retrieved from https://www.ooredoo.com/en/media/news_ view/ooredoo-becomes- the-first-operator-in-myanmar-to-collaborate-with-google-for-a-digital-literacy-and-citizenship-training-program/

Pal, S. K. (2008, June 17). *21st Century Information Technology Revolution*. Ubiquity. Retrieved from https://ubiquity.acm.org/article.cfm?id=1399619

Peciuriene, J. (2017, June 19). *Cyber violence is a growing threat, especially for women and girls*. European Institute for Gender Equality. Retrieved from https://eige.europa.eu/news/cyber-violence-growing-threat-especially-womenand-girls

Rouse, M. (2020, December). *Defination of Cybercrime*. SearchSecurity. Retrieved from https://searchsecurity.techtarget.com/definition/cybercrime

Sobers, R. (2020, October 26). *110 Must-Know Cybersecurity Statistics for 2020*. Varonis. Retrieved from https://www.varonis.com/blog/cybersecuritystatistics/#crime

Staff, P. E. (2018, March 29). *The evolution of cybercrime*. Packt Hub. Retrieved from https://hub.packtpub.com/the-evolution-cybercrime/

Sai Saw Lin Tun. (2014, June 19). *Country Report of Myanmar*. United Nation Economic and Commission for Asia and the Pacific (UNESCAP). Retrieved from https://www.unescap.org/sites/default/files/Myanmar_ppt.pdf

Sreehari, A., Abinanth, K.J., Sujith, B., Unnikuttan, P.S., & Jayashree, M. (2018). A Study Of Awareness Of Cyber Crime Among College Students With Special Reference To Kochi. *International Journal of Pure and Applied Mathematics*, 119 (16), 1353-1360. Retrieved from https://acadpubl.eu/hub/2018-119-16/1/130.pdf

Soe Hay Mar Oo. (2019). *A Study on the Effect of Social Media on Students' Life Case Study: Female Students of Yangon University of Economics* [Master's thesis]. Retrieved from https://meral.edu.mm/records/1051#.X9BxSNgzaUk

Saw Yi Nanda. (2019, October 31). *Cyber Bay Kin gets out word about cybersecurity threats*. Myanmar Times. Retrieved from https://www.mmtimes.com/news/cyber-bay-kin-gets-out-word-aboutcybersecurity-threats.html

Shadrach, B. (2018, June 21). *Upgrading Myanmar's internet access*. Myanmar Times. Retrieved from https://www.mmtimes.com/news/upgrading-myanmarsinternet-access.html

Thinn Thinn Aye. (2012). ICT Development in Myanmar (1988-2010). *Journal of Myanmar academy of arts and science,* X (10), 1-3. Retrieved from https://meral.edu.mm/record/520/files/ICT%20Development%20in%20Myanmar.pdf

Thinn Thinn Aye. (2012). ICT Development in Myanmar (1988-2010). *Journal of Myanmar academy of arts and science,* X (10), 2. Retrieved from

https://meral.edu.mm/record/520/files/ICT%20Development%20in%20Myanmar.pdf

Telenor Myanmar (n.d). *Lighthouse Digital literacy.* Telenor Myanmar. Retrieved from https://www.telenor.com.mm/en/about/digital-literacy

The Nation Thailand. (2017, Jan 9). *Myanmar kids being cyber-bullied: report.* The Nation Thailand .Retrieved from https://www.nationthailand.com/news/30303744

Thaung Htwe & Kyaw Naing Latt. (2017, June 29). *Regional Conference on Cybercrimes 2017.* Department Of Justice. Retrieved from https://www.doj.gov.ph /files/OOC/OOC%20 %20TOT/Cybercrime%20Situation%20in%20Myanmar.pdf

Thiha. (2017, May 1). *Cyber Security Survey Highlights Risks Facing Myanmar's New Internet Users*. Consult-Myanmar. Retrieved from https://consultmyanmar.com/2017/05

UNFPA (Myanmar). (2015, May). *The 2014 Myanmar Population and Housing Census, Yangon Region* (Report No. Census Report Volume 3 – L).UNFPA. Retrieved from https://myanmar.unfpa.org/sites/default/files/pub-pdf/Yangon%20Region%20Census%20Report%20-%20ENGLISH.pdf

Viswanathan, S. T. (2001). Bharat's the Indian cyber laws with cyber glossary (2nd ed.). New Delhi: Bharat Law House.

Venkatasubbarao, M. (2013, May 13). *Professional attitudes of librarians towards information and communication technology: a survey of engineering college libraries in north coastal Andhra Pradesh.* Shodhganga. Retrieved from http://hdl.handle.net/10603/8693

Vapulus. (2018, December 25). *Cyberspace Advantages and Disadvantages*.Vapulus. Retrieved from https://www.vapulus.com/en/cyberspace-advantages-and-disadvantages/

Wright, J.P. (2009). *Rational Choice Theories*. Oxford Bibliographies. Retrieved From https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0007.xml

Yangon Stock Exchange. (n.d.). Myanmar Telecommunications Sector. Retrieved from https://ysx-mm.com/wp-content/uploads/2018/09/Myanmar-Telecommunications-Sector-ENG.pdf

Ye Naing Moe. (2018, Nov 30).*Review on Current Status of Cyber Security in Myanmar* [Video]. YouTube.https://www.youtube.com/ watch?v= OPZ Oq4k_6kQ&t=369s

Zaw Moe Thauk. (2010). Progress of ICT sector contributes to change of lifestyle in Myanmar society. *The New Light of Myanmar,* 18 (193), 6-7. Retrieved from http://www.burmalibrary.org/docs09/NLM2010-10-31.pdf

Website:

https://www.president-office.gov.mm

https://www.mmtimes.com

https://www.refworld.org

https://www.moi.gov.mm

https://thevoicejournal.com

https://theinclusiveinternet.eiu.com

https://www.charltonsmyanmar.com

https://www.itu.int

https://www.irrawaddy.com

https://jsis.washington.edu

https://oxfordbusinessgroup.com

https://www.mlis.gov.mm

https://www.myanmartradeportal.gov.mm

https://www.sydney.edu.au

https://pcdreams.com.sg

http://cybercrime.org.za

https://www.cia.gov

https://ftp.academicjournals.org

https://moderndiplomacy.eu

https://www.scribd.com

https://blogs.worldbank.org

https://thefinancialexpress.com.bd

https://dailytimes.com.pk

https://www.cyberscoop.com

https://www.tuw.edu

https://www.weforum.org

https://www.unodc.org

https://www.telegraph.co.uk

https://www.coe.int

https://www.stalkingriskprofile.com

https://www.statista.com

https://pdf.ic3.gov

APPENDIX

A STUDY ON CYBERCRIMES AWARENESS OF INTERNET USERS IN YANGON

Survey Questionnaire

Section (1) Characteristics of Respondents

1. Gender

   ☐Male ☐Female

2. Age Of Respondents

   ☐ 10 -15 ☐16-20 ☐21-25 ☐29-30

   ☐31-35 ☐36-40 ☐41-45 ☐46-50

   ☐50 and above

3. Educational level of respondent

   ☐Graduate ☐University ☐High School

   ☐Primary School

4. Respondent's Occupation

   ☐Employee ☐Dependence ☐Self-Service

   ☐Students

Section (II) Respondents Internet Services usage types

1. How Many Hours do you Online in a day?

   ☐1 to 5 Hours ☐6 to 10 Hours ☐11 to 15 Hours

   ☐More than 16 hours

2. What types of email do you use in your Daily Life?

☐Office Email ☐Personal Email

☐Office & Personal Email ☐Not Using Email

3. Do You Use Internet Banking services?

☐Using ☐Not Using

4. Select the Social Media that you use the most

☐Facebook ☐Instagram ☐VK ☐Twitter

☐LinkedIn ☐Snap Chat ☐Reddit

5. Select one of the cybercrime case that you know the most?

☐Fraud ☐Cyberbullying ☐Cyber harassment ☐Hacking

☐Virus ☐Child pornography

Section (III) Respondents Awareness Section (Knowledge Questions)

Knowledge Questions	Yes	No
2. Do you know that close relationship with a stranger on online is dangerous?	☐	☐
3. Do you think that your privacy & information are safe by using all in one password for all accounts?	☐	☐
4. Do you know that Public Wi-Fi is not safe for online banking transition?	☐	☐
5. Do you know that sharing privacy & private information on social media and chat rooms is a risk to become cyber victims?	☐	☐
6. Do you know that password leaking can occur when you click the link that someone shares or sends online?	☐	☐
7. Do you know that using Crack & Patch software can be infected viruses, abuse your data and computer system damage as well?	☐	☐
8. Are basic cybercrimes awareness trainings or campaigns very needed to avoid potential cybercrimes?	☐	☐

Section (IV) Actual Practices Question

Actual Practices Questions	Yes	No
1. Have you ever stay closely related to strangers on social media like your close friends?	☐	☐
2. Do you use all in one password for all your accounts?	☐	☐
3. Have you ever used public Wi-Fi for your banking transition?	☐	☐
4.Do you used to share your information on social medias and chatting rooms?	☐	☐
5.Have you ever click the link that shares or send on social media, email, and online?	☐	☐
6.Do you use crack & Patch software at your business?	☐	☐
7. Have you ever attended training or campaigns for cybercrimes awareness or other related cyber security?	☐	☐

Section (V) Knowledge on rule and regulation

1. Does Myanmar have laws to punish cyber criminals?

   ☐Yes ☐No ☐ don't know if have or not

2. Please write down related cybercrimes laws that you know.

Section (VI) Cybercrimes Experiences

Cybercrimes Experiences Questions	Myself	Friends	Medias	No Experience
1. Have you ever experience online financial fraud? **(Fraud)**	☐	☐	☐	☐
2. Have you ever experience on Website and computer network attack? **(hacking)**	☐	☐	☐	☐
3. Have you ever experience your password and your account have been stolen and used by someone? **(Identify theft)**	☐	☐	☐	☐
4. While you are using the internet, have you ever experience the notification message that your devices have infected by a virus or your devices were low performance? **(Scamming)**	☐	☐	☐	☐
5. Have you ever experience on virus infected to your computer and IT devices? **(Virus)**	☐	☐	☐	☐
6. Have you ever received an email with an attachment that sends by a strange address and a stranger one? **(Ransomware)**	☐	☐	☐	☐
7. Have you ever seen something interesting sent to your email, such as a promotion, from a site you do not know? **(Spamming)**	☐	☐	☐	☐
8. Have you ever experience a phone call or a text message by fraudulent communications, such as by email or by a real company? **(Social engineering)**	☐	☐	☐	☐
9. Have you ever experience a message on your browser such asyou are lucky, you won iPhone or something, etc.? **(Malvertising)**	☐	☐	☐	☐
10. Have you ever experience obscene messages and photos that had send by another person or experience someone had been using your photo on other obscene websites or media? **(Cyber harassment)**	☐	☐	☐	☐
11. Have you ever experience spreading your gossip on social media or threatening	☐	☐	☐	☐

coercion by email, text message, and chat room?**(Cyberbullying)**				
12. Have you ever experienced online child sexual abuse and child sexual exploits photos on obscene websites or media? **(Child Pornography)**	☐	☐	☐	☐
13. Have you ever experienced a fraudulent email that acts like a legitimate company or organization and asks for your information about your card number or password?**(Phishing)**	☐	☐	☐	☐