

CRIMINOLOGY OF
CYBER CRIME BEHAVIOR DURING
PANDEMIC COVID-19
IN MALAYSIA

NURUL SYAFIQAH BINTI SAMSU

Bachelor of Computer Science
(Computer System & Networking) With Honors

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : NURUL SYAFIQAH BINTI SAMSU

Date of Birth : 24TH MAY 1998

Title : CRIMINOLOGY OF CYBERCRIME BEHAVIOUR DURING PANDEMIC
COVID-19 IN MALAYSIA

Academic Session : SEMESTER II SESSION 2021 / 2022

I declare that this thesis is classified as:

- CONFIDENTIAL (Contains confidential information under the Official Secret Act 1997)*
- RESTRICTED (Contains restricted information as specified by the organization where research was done)*
- OPEN ACCESS I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:



(Student's Signature)

980524-06-5662
New IC/Passport Number
Date: 01 JUNE 2022



(Supervisor's Signature)

Dr. Syifak Binti Izhar Hisham
Name of Supervisor
Date: 16 JUNE 2023

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

THESIS DECLARATION LETTER (OPTIONAL)

Librarian,
Perpustakaan Universiti Malaysia Pahang,
Universiti Malaysia Pahang,
Lebuhraya Tun Razak,
26300, Gambang, Kuantan.

Dear Sir,

CLASSIFICATION OF THESIS AS RESTRICTED

Please be informed that the following thesis is classified as RESTRICTED for a period of three

Author's Name : Nurul Syafiqah Binti Samsu

Thesis Title : Criminology of Cybercrime Behaviour During Pandemic Covid-19 in Malaysia

Reasons (i)
(ii)
(iii)

(3) years from the date of this letter. The reasons for this classification are as listed below.

Thank you.

Yours faithfully,



(Supervisor's Signature)

Date: 16 JUNE 2023

Stamp:



Note: This letter should be written by the supervisor, addressed to the Librarian, *Perpustakaan Universiti Malaysia Pahang* with its copy attached to the thesis.

SUPERVISOR'S DECLARATION

I/We* hereby declare that I/We* have checked this thesis/project* and in my/our* opinion, this thesis/project* is adequate in terms of scope and quality for the award of the degree of Bachelor of Computer Science in Computer System & Networking



(Supervisor's Signature)

Full Name : Dr. Syifak Binti Izhar Hisham

Position :



DR. SYIFAK BINTI IZHAR HISHAM
HEAD OF PROGRAM (COMPUTER SYSTEMS & NETWORKING)
FACULTY OF COMPUTING
COLLEGE OF COMPUTING & APPLIED SCIENCE
UNIVERSITI MALAYSIA PAHANG
26600 PEKAN, PAHANG DARUL MAKMUR
TEL : 09-424 4604 FAX : 09-424 4666

Date : 16 JUNE 2023

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.



(Student's Signature)

Full Name : NURUL SYAFIQAH BINTI SAMSU

ID Number : CA19020

Date : 03 FEBRUARY 2023

CRIMINOLOGY OF
CYBER CRIME BEHAVIOR DURING
PANDEMIC COVID-19
IN MALAYSIA

NURUL SYAFIQAH BINTI SAMSU

Thesis submitted in fulfillment of the requirements
for the award of the Bachelor of Computer Science in
System and Networking

Faculty of Computer Science
UNIVERSITI MALAYSIA PAHANG

FEBRUARY 2023

ACKNOWLEDGEMENTS

Alhamdulillah, I am grateful and would like to express my sincere gratitude to my supervisor Mrs Syifak Binti Izhar Hisham for her valuable guidance, continuous encouragement and support in doing this research. I really appreciate her guidance from the initial to final level that enabled me to develop understanding of this research thoroughly. Without her advice and assistance, it would be a lot tougher to completion. I also sincerely thanks for the time spent in correcting my mistakes.

My sincere thank go to all lecturers and members of the staff of the Computer System and Networking Department, Universiti Malaysia Pahang, who helped me in many ways and made my education journey at UMP unforgettable. A very thankful for my friends Nur Munirah, Mahligai, Nabilla Natasya, Balqis, Nurul Aqila and Khalil Zulidham for inspiration and support during this completion of research. This three-year experience with them will be remembered as an important memory for me to face a new chapter of life as an engineer.

Then I would like to thank my parents for their love, support and sacrifice throughout my life. Their sacrifice has inspired me from the day I learned how to read and write until what I have become now.

ABSTRAK

Pada zaman moden ini, semakin banyak perkembangan teknologi, hingga menyebabkan hampir 90 peratus rakyat Malaysia menggunakan teknologi dalam kehidupan mereka. Kemudahan aplikasi telefon pintar telah menyebabkan kita mendedahkan maklumat peribadi tanpa disedari dalam alam maya. Akibatnya, maklumat peribadi kita telah dicuri oleh mereka yang tidak bertanggungjawab dan cuba mengambil kesempatan atas kecanggihan teknologi yang ada pada hari ini. Keadaan ini menyebabkan kita terperangkap lalu menjadi mangsa jenayah siber. Antara perlakuan jenayah serta masalah sosial adalah seperti pornografi, penipuan, pelacuran, penyeludupan, peras ugut, pelaburan haram, aktiviti seks bebas, rogol, mencabul kehormatan, penyalahgunaan dadah dan sebagainya. Masyarakat perlu berwaspada terhadap trend terkini jenayah siber melibatkan unsur-unsur '*scam*' atau penipuan yang boleh menyebabkan kerugian mencecah puluhan ribu ringgit kepada mangsa. Kerugian membabitkan jenayah siber sering berkait rapat dengan angka kerugian yang besar berbanding kerugian jenayah harta benda terutama apabila kegiatan itu berselindung di sebalik pekerjaan. Oleh itu kita perlu mengenal pasti modus operasi yang dilakukan oleh kumpulan penjenayah siber ini agar dapat kita hindari dan jauhi daripada terjebak dalam perangkap mereka.

ABSTRACT

In this modern age, there are more technological developments, causing almost 90 percent of Malaysians to use technology in their lives. The convenience of smartphone applications has caused us to disclose personal information unknowingly in cyberspace. As a result, our personal information has been stolen by irresponsible people and try to take advantage of the sophistication of technology available today. This situation causes us to be trapped and become victims of cybercrime. Among the criminal acts and social problems are pornography, fraud, prostitution, smuggling, extortion, illegal investment, free sex activities, rape, indecency, drug abuse and so on. The public needs to be vigilant against the latest trend of cybercrime involving elements of 'scam' or fraud that can cause losses of tens of thousands of ringgits to victims. Losses involving cybercrime are often closely linked to large loss figures compared to property crime losses especially when the activity is disguised behind employment. Therefore, we need to identify the mode of operation performed by this group of cyber criminals so that we can avoid and stay away from getting caught in their trap.

TABLE OF CONTENT

DECLARATION	
TITLE PAGE	
ACKNOWLEDGEMENTS	7
ABSTRAK	8
ABSTRACT	9
TABLE OF CONTENT	10
LIST OF TABLES	13
LIST OF FIGURES	14
CHAPTER 1	16
INTRODUCTION	16
1.1 Introduction	16
1.2 Problem Statement	17
1.3 Objective	19
1.4 Scope	19
1.5 Significant	20
1.6 Report Organization	21
CHAPTER 2	22
LITERATURE REVIEW	22
2.1 <i>Introduction</i>	22
2.2 <i>Overview</i>	22
2.3 <i>Situational Crime Prevention (SCP)</i>	23
2.3.1 Routine Activity Theory	24
2.3.2 Crime Pattern Theory	24
2.3.3 Rational Choice Perspective	25

2.4	<i>Comparison Between Three Theories</i>	25
2.5	<i>Summary of the theories</i>	26
CHAPTER 3		27
METHODOLOGY		27
3.1	<i>Project Management Framework</i>	27
3.1.1	Research Design	27
3.1.2	Sampling Design	28
3.1.3	Research Instrument	28
3.1.4	Data Analysis	28
3.2	<i>Project Requirement</i>	28
3.2.1	Input	28
3.2.2	Output	28
3.2.3	Process Description	28
3.2.4	Constraints and Limitations	29
3.2.5	Software Requirement	29
3.2.6	Hardware Requirement	30
3.3	<i>Proposed Design</i>	31
3.4	<i>Data Design</i>	32
3.5	<i>Proof of Initial Concept</i>	33
3.6	<i>Methodologies Plan</i>	35
3.7	<i>Potential Use of Validation Plan</i>	35
CHAPTER 4		37
IMPLEMENTATION, RESULT AND DISCUSSION		37
4.1	<i>Introduction</i>	37
4.2	<i>Implementation Process</i>	37
4.2.1	Research Objective	37
4.2.2	Research Question	37
4.2.3	Findings of the study	37

4.2.4	Demographic profile	38
4.2.5	Parenting Observation	40
4.2.6	Cyber crime Experience	42
4.2.7	Threat Severity Cyber crime	44
4.2.8	Self-Efficacy	45
4.3	<i>Testing and Result Discussion</i>	50
4.3.1	Trial of testing for parent observation	51
4.3.2	Trial of testing for cybercrime experience	52
4.3.3	Trial of testing for threat severity cyber crime	54
4.3.4	Trial of Test for Self- Efficacy	55
CHAPTER 5		58
CONCLUSION		58
5.1	<i>Introduction</i>	58
5.2	<i>Research Constraint</i>	58
5.3	<i>Future Work</i>	59
5.4	<i>References</i>	60
5.5	<i>Appendix</i>	62
5.5.1	Gantt Chart	62
5.5.2	Information Data of Output RStudio	63
5.5.3	Coding for RStudio	67
5.5.4	Proof of Survey	72

LIST OF TABLES

Table 1.1 : Summary of problem faced by Malaysia's people	18
Table 2.1 : The comparison of theories	25
Table 3.1: The software Requirement of the Research	29
Table 3.2 : The Hardware Requirement of the Research	30
Table 3.3 : 25 Techniques Situational Crime Prevention (SCP)	34
Table 4.1 : Shows how vigilant parents monitor their kids' technology use.	41
Table 4.2: Show basic information from respondents.	42
Table 4.3: Show respondent's experiences online.	43
Table 4.4: Show the statement about threat vulnerability of respondents.	44
Table 4.5: Show the rating of how good respondents protect their devices.	47
Table 4.6: Cybercrime behavior of participants in online fraud concerns	48

LIST OF FIGURES

Figure 1.1 : shows statistic case Covid-19 of state in Malaysia.	16
Figure 2.1 : Routine Activity Theory	24
Figure 2.2 : Crime Pattern Theory	24
Figure 2.3 : Show the acquisitive crime patterns	26
Figure 3.1 : The Research Methodology	26
Figure 3.2 : Flowchart of questionnaire knowledge responder	31
Figure 3.3 : Dataset of Respondent	31
Figure 3.4 : General Incident Classification Statistics 2020 occurrences	33
Figure 3.5 : Logo of R Project and RStudio	33
Figure 4.1 : Categorized of ages by the respondents	38
Figure 4.2 : Show the percentage of race in Malaysia based on respondents answer	38
Figure 4.3 : Categorized of status by the respondents	39
Figure 4.4 : Show the percentage of occupation respondents in Malaysia.	39
Figure 4.5 : Show the total children according to the married group respondent	40
Figure 4.6 : Show the number of experienced being a victim by respondents	42
Figure 4.7 : Show the experiences of cyber-crime by respondents	43
Figure 4.8 : Show the situation of experiences by respondents	46
Figure 4.9 : Show the rating how respondents get advice about staying online	49
Figure 4.10 : Show the school prepared for dealing with cyber threat	49
Figure 4.11 : Show the result of respondent detail.	50

Figure 4.12 : Result based on parent observation	51
Figure 4.13 : First trial testing of cyber crime experience	52
Figure 4.14 : Second Trial of cyber crime experiences	53
Figure 4.15 : Result of trial testing for threat severity cyber crime	54
Figure 4.16 : First trial testing for self-efficacy	55
Figure 4.17 : Second trial testing for self-efficacy	57
Figure 5.1 : The process of PSM	62
Figure 5.2 : Summary Coding for Parenting Observation	63
Figure 5.3 : View detail of Parenting Observation Data	63
Figure 5.4 : Summary Coding for Cyber Crime Experience	62
Figure 5.5 : View detail of Cyber Crime Experience Data	62
Figure 5.6 : Summary Coding for Threat Severity Cyber Crime	62
Figure 5.7 : View detail of Threat Severity Cyber Crime Data	62
Figure 5.6 : Summary Coding for Self-Efficacy	62
Figure 5.7 : View detail of Self-Efficacy Data	62

CHAPTER 1

INTRODUCTION

1.1 Introduction

The latest data from the Malaysian Ministry of Health reports that covid-19 virus has currently invaded Malaysia with infecting 2,492,343 people and causing 96,099 confirmed deaths, although 2,396,244 covid-19 patients have recovered. The last week case is alarming because every day reported more than 3 thousand new cases of infected people. Indeed, if quantitatively compared to the world's population of about 7.8 billion, the casualties seem small but of course it is not as simple to conclude if we look at the case from every state, from every city.

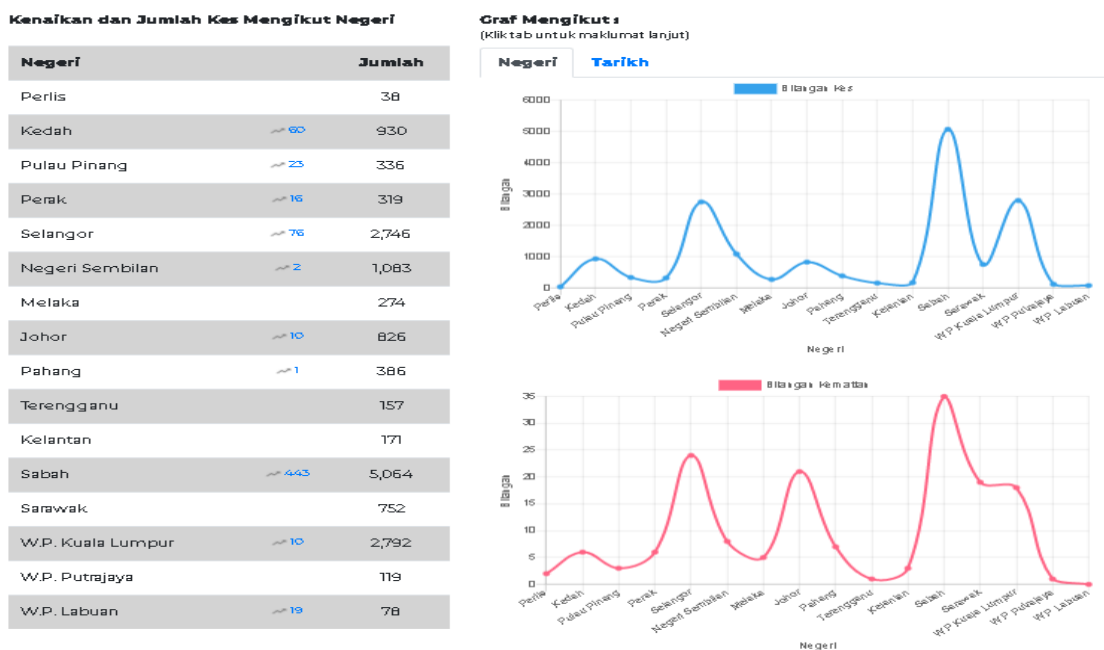


Figure 1.1 : shows statistic case Covid-19 of state in Malaysia.

Looking at the brief data above, it is not an exaggeration to say that the covid-19 pandemic has had an unprecedented impact on the world, without exception. Not apart from the impact of this pandemic is the crime rate and the map distribution (crime distribution rate) in various parts of the world, both street crime (street or predatory crimes), as well as white collar crime (white collar crime), individual crime and organized crimes, both crimes against persons and property crimes. One of the key variables agreed upon as a very decisive variable in the number and distribution of crime during this pandemic is the government's policy on social distancing, lockdown, work from home, which in our country is modified into Large -Scale Social Restrictions (PSBB). To limit the spread of COVID-19, this government regulation urges locals to stay their distance. Of course, the policies that are transformed in this kind of order in each country are different, some are accompanied by strict legal sanctions, and some are simply given social sanctions.

1.2 Problem Statement

Cyber crime complaints increased 99.5% to 20,805 during the COVID-19 outbreak from 10,426 in 2019, according to crime statistics from the Department of Statistics Malaysia (**DoSM**). DoSM says that the number of complaints about false elements went up by 117.6%, or 6,637, compared to the number of complaints in 2019, which was 3,050. However, despite the increase in cybercrime, physical crime decreased last year by 21.4% to 65,623 cases compared to 83,456 cases in 2019. Violent crime recorded a decrease of 19.5% to 13,279 cases while property crime decreased 21.8% to 52,344 cases. This drop in crime is due to a number of Movement Control Orders (**MCO**) that put limits on social activities and travel across country lines and borders. The spread of Covid-19 has caused Malaysia's people to be disrupted to carry out various activities due to having to carry out Large -Scale Social Restrictions (**PSBB**) as well as SOP Movement Control Order (**MCO**) instructions from the National Security Council (**NSC**) which is very long and staged. This has led to Malaysians doing their jobs and schoolwork from home, potentially making them targets for cyber criminals. As a result, during the epidemic, some people take advantage of the increased usage of web services to promote ideology and perpetrate crimes. Most cases are money loans, SMS fraud, unpaid debt phone lines, and other types of fraud that can cost Malaysians hundreds of thousands of ringgits, cyberbullying, hacking, spam, and cyber intrusions.

Table 1.1 : Summary of problem faced by Malaysia's people

No	Categorized	Problem	Effect
1.	Student or teenager	Commit cybercrime just for fun or perform small actions such as hacking passwords to get revenge on their teachers or friends.	May cause cyberbullying such as harassment or defamation of others.
2.	Children	Children who are still naive are exposed to widespread sexual exposure on online gaming platforms.	Can make that child addicted to pornography.
3.	Adult	Make many online transactions for online platforms or buy from independent sellers who use third party sites without checking the origin.	Victims become blindsided by the cheap prices of products offered through advertisements on social media, at the same time there will be issues of scammer or fraud and loss of money.
4.	Workers	Often use email, blog sites and new technologies to work without any vigilance in doing prevention and how to overcome cybercrime.	It is easy to steal data due to corruption in data and damage to software and computer systems

1.3 Objective

Based on the problem statements, the objectives of the research are:

- I. To understand about criminology and criminal behaviour.
- II. To identify the determine amount of fear of crime, security, and preventive action based on responses.
- III. To analyse applicable prevention techniques that has been taken based on responder.

1.4 Scope

I. User Scope

- A. Students aged 9 to 17 years old who are exposed to mobile application.
- B. Adults people that obsess with shopping online and use modern technologies.

II. Survey Scope

- A. Defined people's general knowledge about information of cybercrime behaviour.
- B. Define based on the unique position of people that will be investigated using technologies to identify whether the difference in circumstances lead to specific results.

III. Development Scope

- A. Online Survey Method (Google Form)
- B. RStudio tool
- C. R Project Programme

1.5 Significant

I. Children

Children can be given early exposure to the use of this increasingly sophisticated technology. So, they can use these technologies well in the future.

II. Parents / Adults

Parents can teach or observe the behaviour of their children's newly introduced technologies so as not to be affected by unwanted things at home. Adults can protect their computer and personal data in the best ways.

III. Student

Students can reduce cyberbully cases by being given early prevention from the school or family.

IV. Employee

Employees can prepare or precautions in dealing with cyber issues without any problems as well as not bothering the workplace.

1.6 Report Organization

There are three chapters in this thesis:

1. Chapter 1

In this chapter, the researcher is discussing about the introduction of criminology of cybercrime behaviour during Pandemic Covid 19 in Malaysia. Then, the researcher explains about the problem statement that need to be developed. This thesis can achieve in this chapter by discover the problem statement, objective, scope, and significance of the research.

2. Chapter 2

Chapter 2 briefly explains about the literature review on criminology of cybercrime behaviour during pandemic COVID-19. The researcher also discussed three theories method that have been used to prove to diminish crime by suing Situational Crime Prevention. At the end of this chapter, the researcher is come out with the comparison between three theories that are related to this thesis.

3. Chapter 3

In chapter 3, the researcher discussed the methodology for criminology of cybercrime behaviour during pandemic COVID-19. This project implements a research framework methodology. The stages that are used in this project are Input, Output, Process description, Constraints and limitations, and Case study.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

As the usage and trust on information technology becomes more widespread in society, so does the targeting and exploitation of computer systems. With more than one-fourth of the world's population utilising the Internet, learning how to be safe online is becoming extremely important. Because of the speed, ease, and anonymity of the internet, cyber crime is becoming a rapidly rising activity. According to one recent research, one out of every five people has had personal information stolen or an account compromised because of their online activity. Aside from online identity theft and financial fraud, cyber crime may also include information piracy, forgeries, email spoofing, stalking, bullying, and intellectual property crimes. With so many possible hazards online, there are solutions to secure of people, children, and employee information from cyber thieves. After all, cybercrime cannot be entirely eradicated. However, it is occasionally preventable. It all begins with developing strong internet safety practices. Here are some theories to help people better defend themselves against cyber crime.

2.2 Overview

A research study of a few references on information cyber crime behaviour prevention will be presented depth in this chapter, which is a literature review. There are five subtopics under this chapter. In *subtopic 2.1* has been discussed in detailed about criminology of cybercrime. In *subtopic 2.3* will review three existing theories that is related to this research. After that, the comparison between three theories has been discussed under *subtopic 2.4*. Lastly, in *subtopic 2.5*, the summary for the best three theories has been discussed for future used in cybercrime behaviour during pandemic covid 19 in Malaysia.

2.3 Situational Crime Prevention (SCP)

Situational Crime Prevention (SCP) is a criminological method that is proved to diminish crime opportunities drawing from five main tactics containing 25 approaches. With global cybercrime rising, practitioners and scholars are exploring SCP tactics and strategies to prevent malware and cyber-enabled crimes. Recent study suggests that SCP can be used to combat cybercrime. However, most of this research employs only a handful of the SCP strategies, and the SCP tactics and cybercrime reduction are seldom linked. In this work, we assess the applicability of the whole range of SCP cybercrime methods and describe how computer scientists, cybersecurity researchers, and practitioners employ SCP principles to prevent and control cybercrime. This study defines terminology, investigates the increase of cybercrime, and discusses the significance of SCP for reacting to cybercrime using a targeted systematic review of 352 papers from the computer science, criminal justice, and criminology literature using the PRISMA approach. The researchers summarise SCP research on cybercrime and propose research gaps and future areas.

SCP was developed in the 1970s by researchers at the British government of criminal research department, the Home Office Research Unit. It was defined as an event-focused strategy to reducing criminal possibilities. SCP began as a collection of strategies aimed at certain types of crime that changed crime event conditions to lessen the likelihood of crimes occurring. Clarke (1995) developed 12 SCP approaches in 1992, which were divided into three broad tactics. Clarke and Homel expanded these to 16 SCP approaches (grouped by four main tactics) (1997). Cornish and Clarke (2003) then revised the list again, resulting in the present 25 SCP approaches. Figure 2 depicts the genealogical evolution of SCP approaches. Next, the five SCP general strategies and 25 SCP techniques are explained. Three criminological theoretical approaches are nicely aligned with SCP principles: (i) routine activity theory, its original version described how macrosocial changes created macro criminal chances; (ii) crime pattern theory, which discusses environmental impacts and dynamic layers of travel at the highest level and how neighbourhood characteristics affect crime possibilities; and (iii) the rational choice which works on a small scale and shows how decisions are made at the individual level.

2.3.1 Routine Activity Theory

Routine activity theory is very closely connected with the ideas of Situational Crime Prevention and has led to several theoretical insights that have helped come up with solutions to crime-related problems over time. Work on the journey-to-crime utilising the idea of everyday activities, for example, is a very important ally for SCP in explaining how offenders and targets meet without guessing on their motives.



Figure 2.1 : Routine Activity Theory

2.3.2 Crime Pattern Theory

Similarly, crime pattern theory proposes that criminals exploit crime possibilities based on their activity and understanding of places during routine trips to nodes (such as work, school, and home). When these people's movement patterns and the physical environment come together, they create "*criminogenic environments*" that the SCP can change to make it less likely that crime will happen. Crime pattern theory indicates that offenders are more likely to commit crimes when their consciousness zone crosses with eligible victims.

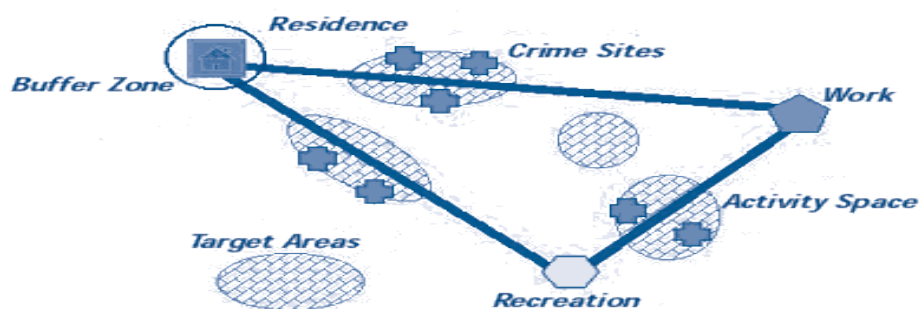


Figure 2.2 : Crime Pattern Theory

2.3.3 Rational Choice Perspective

These three ideas tell that the important things about how chance blocking works that are relevant to SCP. In rational choice theory, for example, people are considered to make judgments about when, how, and where to commit crimes when the circumstances are beneficial to them. Goal of creating adverse circumstances for SCP is thus discovered to dissuade sensible individuals from breaking the law. Indeed, rational choice theories never condemn a criminal act as wanton, dumb, or senseless but seek to understand the offender's aims. Rational choice theory examines how an offender makes criminal choices based on a motivation in a situation that provides possibilities to fulfil that goal. The red circle shows where these two people are likely to commit a crime.

2.4 Comparison Between Three Theories

Table 2.1 : The comparison of theories

	ROUTINE ACTIVITY THEORY	CRIME PATTERN THEORY	RATIONAL CHOICE PERSPECTIVE
Author	Cohen and Felson 1979	Brantingham 1993	Clarke and Cornish 1985, Cornish and Clarke 1986
Benefit	Each effectively committed violation demands at the very least an offender with criminal tendencies as well as the competence to carry out those impulses.	This theory aids law enforcement in figuring out why crime exists in certain areas. It helps predict where certain crimes may occur.	States that humans use rational calculations to make rational choices.
Limitation	When a crime is stopped, it frequently takes time and effort to discover a new way to offend.	Offenders go no farther than they need to and do not use unusual methods to travel	It emphasises individual activity. Individual activity drives huge social formations, yet this explanation is limited.
Environmental	Suitable target, Motivated Offender, and absence of capable guardian.	Nodes, Path, Edge	Victim, offender

2.5 Summary of the theories

In this chapter, three theories that have been applied to implement the cybercrime prevention have been reviewed and discussed in detail. Then, the comparison between the three theories have been discussed. For the information cybercrime prevention will be used is based on the advantages of three existing theories.

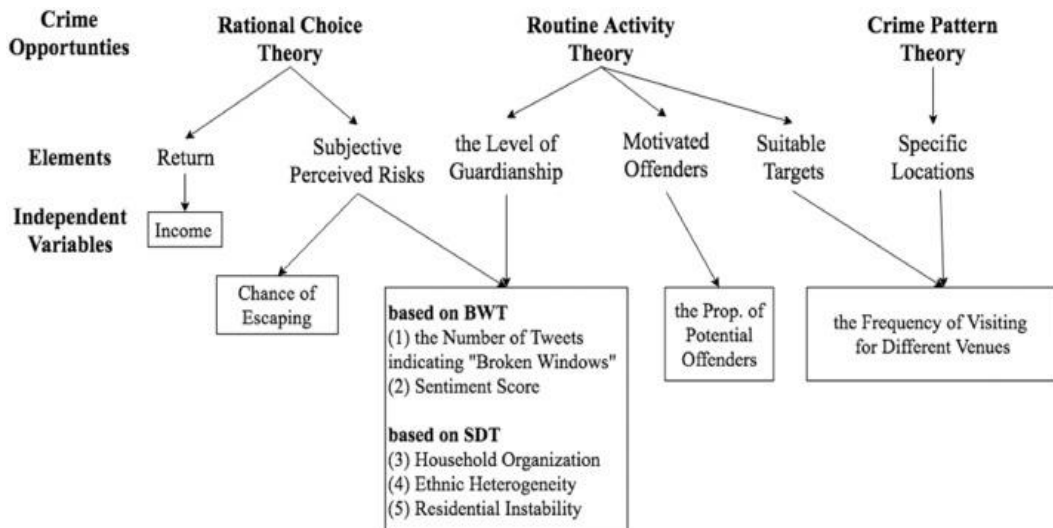


Figure 2.3 : Show the acquisitive crime patterns

CHAPTER 3

METHODOLOGY

3.1 Project Management Framework

This section will describe the methodology to be used. There are many methodologies that can be defined but for this research will focus on Research methodology where to do any practical part of the “*how*” of research. More precisely, it concerns the way researchers plan studies methodically to produce accurate and reliable results that address the goals and objectives of the research. In this chapter, a detailed explanation will be given on prevention techniques as well as the features for this thesis.

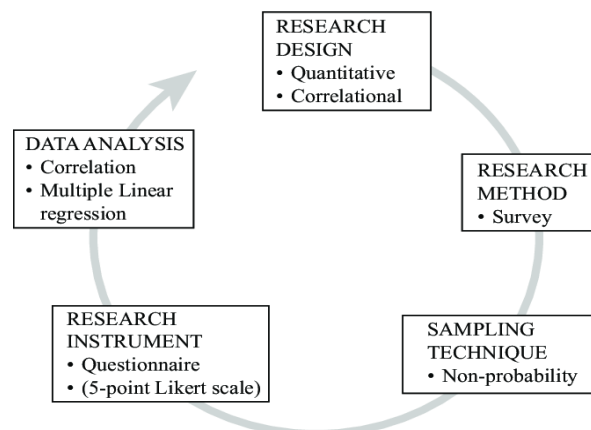


Figure 3.1 : The Research Methodology

3.1.1 Research Design

The quantitative approach will be used for this thesis. This is a type of research that focuses on objective things and is controlled by collecting and analysing data. A type of research in which variables are measured with scientific and experimental tools. The RStudio test is used in a study to try to explain, explain, or find the relationship between the variables. This study is an inferential study, and the scores the respondents gave will be changed from a Likert scale to an interval scale so that multiple linear regression analysis can be used as a test tool. So, 150 responder of Malaysia people or more will be answer the questionnaire to get the actual data.

3.1.2 Sampling Design

Instead of random sampling, the sampling design for this thesis will be based on the idea of non-probability sampling. This is because this thesis will probably use convenience samples, like surveys of people that have access to, like friends, family, or co-workers, instead of a completely random sample, which may be hard to reach because of limited resources. Most of the time, it cannot generalise the results of non-probability sampling.

3.1.3 Research Instrument

There are different ways to collect information for this thesis. Interviews (which can be unstructured, semi-structured, or structured), surveys (online or in person), observation, documents and records, and case studies are all ways to look at these possibilities. But the way data is collected will depend on the overall goals and objectives of this thesis, as well as how practical it is. This thesis is meant to be exploratory, by quantitative methods which mean using questionnaire survey method. On the other hand, if the research wants to measure specific variables or test hypotheses, it might want to use large-scale surveys that produce a lot of numbers.

3.1.4 Data Analysis

Analysis techniques are categorised according to whether the research question is quantitative in nature. In quantitative research, the methods of descriptive and inferential statistics are often used to analyse data. In this thesis, the goals, and objectives, as well as the practicalities and resource constraints, dictate how data is collected.

3.2 Project Requirement

3.2.1 Input

The input data is the dataset that will be taken from questionnaire of survey that been answer from respondents.

3.2.2 Output

Output for this is data after processing that have been collected. All the result of survey will be recorded and will determine the best prevention.

3.2.3 Process Description

The complete testing procedure consists of four parts. At begin, to collect this survey thesis, a mixed-method approach, meaning qualitative and quantitative data from Malaysians, is

required. Furthermore, the data that will be collected is a random sample of persons of all races and ages. To avoid technical mistakes, clear data and calculate numerous data sets with various tests. To reduce data mistakes, all manipulating variables should be examined as much as feasible. Finally, data analysis is required to determine the accurate test findings.

3.2.4 Constraints and Limitations

The usage of the survey field for Web-Based Survey Tools, which is the Google Form, is a constraint in this thesis. The Google Form can enable the answer to fill in the data entirely unless the user sets it to satisfy the constraint, in which case the reply must rectify it before continuing. Any boundaries or dangers that must be considered throughout the project's life cycle are referred to as constraints in this thesis.

In the meanwhile, Data Protection and Data Security will be limited. Every Google Forms user is responsible for ensuring that replies are aware of and adhere to the fundamental Data protection and security requirements. Human mistake, not technology error, is responsible for most data privacy infractions. As a result, before using Google Forms, users should familiarise themselves with the data protection regulations and functionalities and be aware of these requirements.

3.2.5 Software Requirement

The table shown that software that have been required in this thesis.

Table 3.1: The software Requirement of the Research

Software	Specification	Purpose
Microsoft Office Word	Version 365	Used for the report documentation.
Microsoft Office PowerPoint	Version 365	Used for preparing presentation material.
Microsoft Project	Version 365	Used to make Gantt chart of process finishing project.
Microsoft Edge	Version 102.0.1245.33	Used for opening some document using pdf format.
Opera Browser	Version 66	Being used to do some research regarding to the project.
Draw.io	Version 19.0.0	To draw the flowchart for the thesis.
RStudio	Version 2022.12.0-353	Used for Survey Data analysis

3.2.6 Hardware Requirement

This thesis is identifying hardware for testing. The efficiency and usability of hardware in the face of high-load data are critical and highly required. The hardware necessary for this study is listed in the table below:

Table 3.2 : The Hardware Requirement of the Research

Hardware	Specification	Purpose
Laptop	HP 14s-cf1058TX OS: Window 11 Processor : AMD Ryzen™ 5 5500U (up to 4.0 GHz max boost clock, 8 MB L3 cache, 6 cores, 12 threads RAM : 4 GB DDR4-2400 SDRAM (1 x 4 GB)	Used for documentation, testing, development and research of this thesis.
Smartphone	Samsung A31 CPU : Octa-core (2x2.0 GHz Cortex-A75 & 6x1.7 GHz Cortex-A55) GPU : Mali-G52 MC2 OS : Android 12, One UI 4.1	Used for on recording data and documentation that also produce chart.
Smartphone	Apple iPhone X CPU : Hexa-core 2.39 GHz (2x Monsoon + 4x Mistral) GPU: Apple GPU (three-core graphics) OS : iOS15.5	Used for testing the survey that will be conducted to complete this research.

3.3 Proposed Design

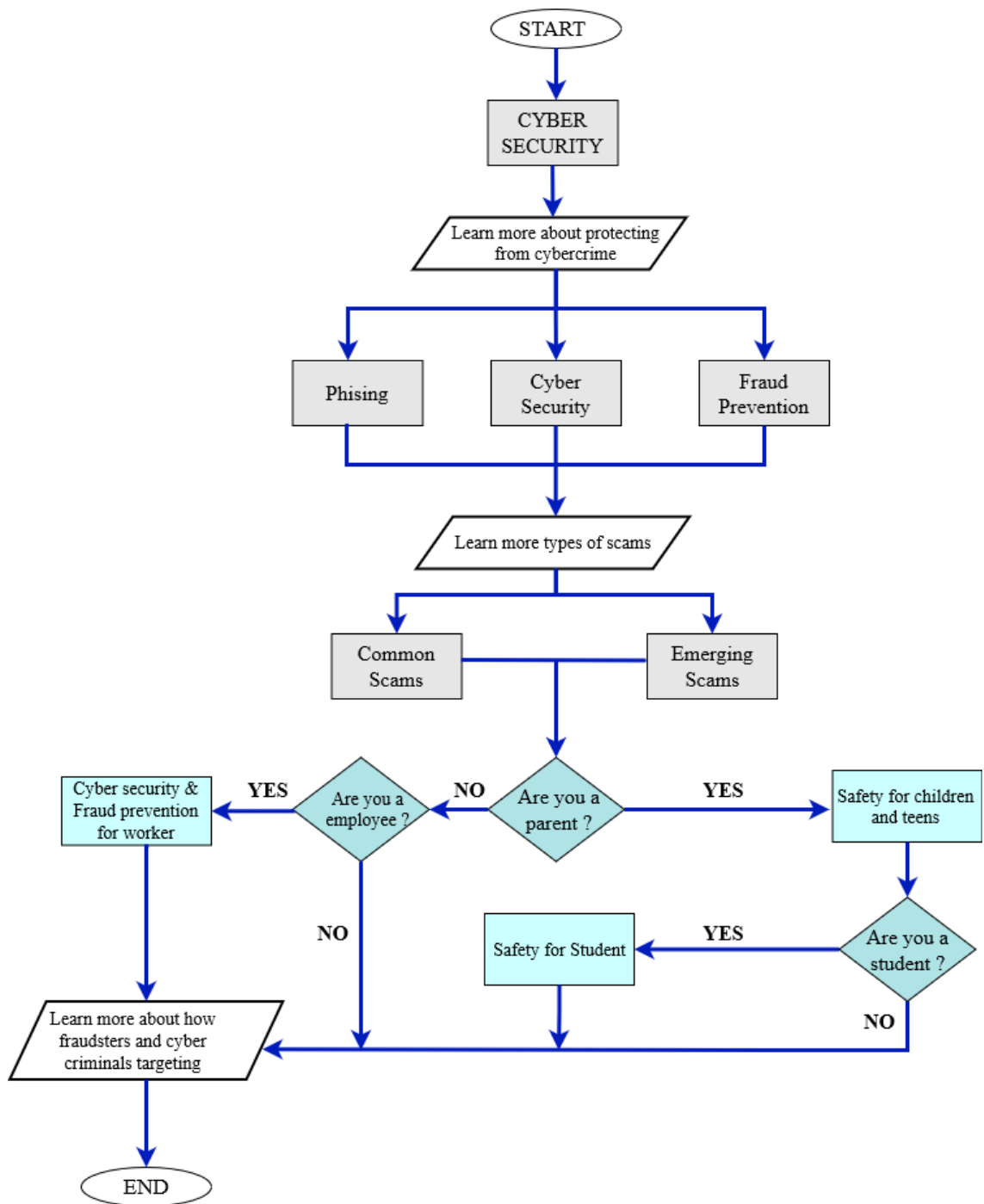


Figure 3.2 : Flowchart of questionnaire knowledge responder

3.4 Data Design

Based on the explanation provided earlier, its state that the data set that will be utilised in this investigation will be obtained from survey that have been taken from responder.

Timestamp	Email	Gender	Age	Race	Status	Occupation	Num_Child	P1	P2	P3	P4	P5	P6	
11/22/202	khallizulidF	Male	18 - 25 years old	Malay		Student	No child	Agree	Agree	Neutral	Agree	Agree	Agree	
11/22/202	syafiqahsai	Female	18 - 25 years old	Malay	Single	Student								
11/22/202	shahmi.sh	Male	18 - 25 years old	Malay	Single	Employed								
11/22/202	farranadial	Female	18 - 25 years old	Malay	Married	Employed	No child	ye	Strongly A ₅	Strongly A ₁	Neutral	Neutral	Strongly A ₅	Strongly A ₅
11/22/202	khallizulidF	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	nurulaqilah	Female	18 - 25 years old	Malay	Single	Student								
11/22/202	sharyramz	Female	9 - 17 years old	Malay	Single	Student								
11/22/202	fikri.j1988	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	samsulmus	Male	36 and above	Malay	Married	Employed	more than 2 - 5 child	Strongly A ₅	Strongly A ₁	Neutral	Strongly A ₅	Neutral	Agree	Agree
11/22/202	izzatiazaha	Female	26 - 35 years old	Malay	Married	Employed		Strongly A ₅	Strongly A ₁	Strongly A ₅	Strongly A ₅	Strongly A ₅	Strongly A ₅	
11/22/202	nuraj2102	Female	18 - 25 years old	Other	Single	Student								
11/22/202	nurnajwa0	Female	18 - 25 years old	Malay	Single	Student								
11/22/202	azerimohd	Male	36 and above	Malay	Married	Employed	2 - 5 child	Agree	Agree	Agree	Agree	Agree	Agree	
11/22/202	mohamadT	Male	18 - 25 years old	Malay	Single	Unemployed								
11/22/202	nurulnabil	Female	18 - 25 years old	Malay	Single	Student								
11/22/202	syazwanI21	Female	26 - 35 years old	Malay	Single	Employed								
11/22/202	anassulhi.r	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	syafiqsams	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	asyrafzainc	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	eyokhairul	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	dnyshahz	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	luqmanhkr	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	qistinaamz	Female	18 - 25 years old	Malay	Single	Student								
11/22/202	zaimhkm2	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	mgtfhm@G	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	samsulhafi	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	mbukhour	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	syafiqaher	Female	18 - 25 years old	Malay	Single	Student								
11/22/202	amalimanZ	Female	18 - 25 years old	Malay	Single	Student								
11/22/202	farahmardI	Female	18 - 25 years old	Malay	Single	Student								
11/22/202	eizzhairai	Male	18 - 25 years old	Malay	Single	Student								
11/22/202	nurulainar	Female	26 - 35 years old	Malay	Married	Employed	1 only child	Agree	Neutral	Agree	Agree	Neutral	Neutral	
11/24/202	ajijiazizi19	Male	18 - 25 years old	Malay	Single	Student								
11/24/202	baihaqqiza	Male	18 - 25 years old	Malay	Single	Student								
11/24/202	m.amiraka	Male	18 - 25 years old	Malay	Single	Student								
11/24/202	impianadill	Female	18 - 25 years old	Malay	Single	Employed								
11/24/202	hazierazair	Female	18 - 25 years old	Other	Single	Student								
11/24/202	amiralokm	Female	18 - 25 years old	Malay	Single	Employed								
11/24/202	imran.shaz	Male	18 - 25 years old	Malay	Single	Employed								
11/24/202	sitinurfazli	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	thaqifrosdi	Male	18 - 25 years old	Malay	Single	Student								
11/24/202	zuhailiazaz	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	rozalinabax	Female	18 - 25 years old	Other	Single	Student								
11/24/202	gajushitam	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	sulaimanbi	Male	18 - 25 years old	Malay	Single	Employed								
11/24/202	najwa3079	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	muhdfirda	Male	18 - 25 years old	Malay	Single	Employed								
11/24/202	jannahaziz	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	syakirrashi	Male	18 - 25 years old	Malay	Single	Employed								
11/24/202	aisyahmoh	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	ainabasyirz	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	iya932175i	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	fadirazulhe	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	haziqqirfar	Male	18 - 25 years old	Malay	Single	Student								
11/24/202	mnhafizah	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	naqib.razaI	Male	18 - 25 years old	Malay	Single	Employed								
11/24/202	tf19014@s	Male	18 - 25 years old	Malay	Single	Student								
11/24/202	amirizwan	Male	18 - 25 years old	Malay	Single	Employed								
11/24/202	zulfawahid	Female	18 - 25 years old	Malay	Single	Employed								
11/24/202	imrantafa	Male	18 - 25 years old	Malay	Single	Student								
11/24/202	nmdihah5	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	fasabri22@	Male	26 - 35 years old	Malay	Single	Employed								
11/24/202	najwazurai	Female	18 - 25 years old	Malay	Single	Employed								
11/24/202	sityrahimal	Female	18 - 25 years old	Malay	Single	Student								
11/24/202	zcrew88@	Male	18 - 25 years old	Malay	Single	Student								

Figure 3.3 : Dataset of respondent

According to the data set shown above, a significant detail of responder will have been recorded between 9 to 35 above year olds. Each reason is explained by referring to the specific illegal conduct that prompted it.

Reported Incidents based on General Incident Classification Statistics 2020

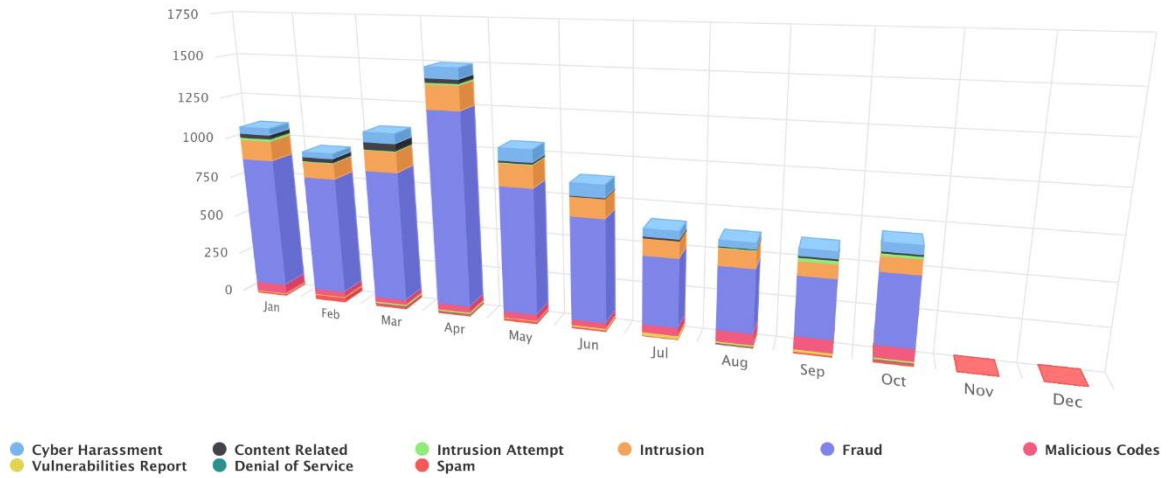


Figure 3.4 : General Incident Classification Statistics 2020 occurrences

The statistical data shown above demonstrates that the current number is higher than the one that was recorded in the year 2019. The most prevalent kind of cyber crime during the time period was fraud, followed by intrusion instances as the second most prevalent type. This demonstrates that the COVID-19 epidemic that occurred this year has made more people who depend on internet technology more susceptible to the danger of cyber assaults.

3.5 Proof of Initial Concept

Throughout the course of this investigation, doing this research in accordance with the Routine Activity Theory, the Crime Pattern Theory, and the Rational Choice Perspective, which are all different viewpoints within the discipline of criminology. Because of this will be able to evaluate the comprehension of respondent by cybercriminal behaviour, which is important given that most of the cyber crime originates from this conceptual theory.

Table 3.3 : 25 Techniques Situational Crime Prevention (SCP)

INCREASE THE EFFORT	INCREASE THE RISKS	REDUCE THE REWARDS	REDUCE PROVOCATIONS	REMOVE THE EXCUSES
1. Target Harden <ul style="list-style-type: none"> ✚ Steering Column locks ✚ Anti-robbery screens ✚ Tamper-proof packaging 	6. Extend Guardianship <ul style="list-style-type: none"> ✚ Take routine precautions ✚ Cocoon neighbourhood watch 	11. Conceal Targets <ul style="list-style-type: none"> ✚ Off-street parking ✚ Gender-neutral phone directories ✚ Unmarked bullion trucks 	16. Reduced Frustration & Stress <ul style="list-style-type: none"> ✚ Efficient queues & polite service ✚ Expanded seating ✚ Soothing music / muted lights 	21. Set Rules <ul style="list-style-type: none"> ✚ Rental agreement ✚ Harassment Codes ✚ Hotel registration
2. Control Access to Facilities <ul style="list-style-type: none"> ✚ Entry phones ✚ Electronic can access ✚ Baggage screening 	7. Assist Natural Surveillance <ul style="list-style-type: none"> ✚ Improved street lighting ✚ Defensible space design ✚ Support whistle-blowers 	12. Remove Targets <ul style="list-style-type: none"> ✚ Removable car radio ✚ Women's refuges ✚ Pre-paid phone cards for pay phones 	17. Avoid Disputes <ul style="list-style-type: none"> ✚ Separate encloses for rival soccer fans ✚ Reduce crowding in pubs ✚ Fixed cab fares 	22. Post Instructions <ul style="list-style-type: none"> ✚ No Parking ✚ Private property ✚ Extinguish campfires
3. Screen Exits <ul style="list-style-type: none"> ✚ Ticket needed for exit ✚ Export documents ✚ Electronic merchandise tags 	8. Reduce Anonymity <ul style="list-style-type: none"> ✚ Taxi driver IDs ✚ How's my driving? Decals ✚ School uniforms 	13. Identify Property <ul style="list-style-type: none"> ✚ Property marking ✚ Vehicle licensing & parts marking ✚ Cattle branding 	18. Reduce Emotional Arousal <ul style="list-style-type: none"> ✚ Controls on violent pornography ✚ Enforce good behaviour on soccer field ✚ Prohibit racial slurs 	23. Alert Conscience <ul style="list-style-type: none"> ✚ Roadside speed display boards ✚ Signatures for customer declarations ✚ Shoplifting is stealing
4. Deflect Offenders <ul style="list-style-type: none"> ✚ Street closures ✚ Separate bathrooms for women ✚ Disperse pubs 	9. Utilise Place Managers <ul style="list-style-type: none"> ✚ CCTV for double-decker buses ✚ Two clerks for convenience stores ✚ Reward vigilance 	14. Disrupt markets <ul style="list-style-type: none"> ✚ Monitor pawn shops ✚ Controls on classified ads ✚ License street vendor 	19. Neutralise Peer Pressure <ul style="list-style-type: none"> ✚ Idiot drink & drive ✚ Its's OK to say NO ✚ Disperse troublemakers at school 	24. Assist Compliance <ul style="list-style-type: none"> ✚ Easy library check-out ✚ Public lavatories ✚ Litter Bins
5. Control Tools / Weapon <ul style="list-style-type: none"> ✚ Smart guns ✚ Disabling stolen mobile phones ✚ Restrict spray paint to juveniles 	10. Strengthen Formal Surveillance <ul style="list-style-type: none"> ✚ Red light cameras ✚ Burglar alarms ✚ Security guards 	15. Deny Benefits <ul style="list-style-type: none"> ✚ Ink merchandise tags ✚ Graffiti cleaning ✚ Speed humps 	20. Discourage Imitation <ul style="list-style-type: none"> ✚ Rapid repair of vandalism ✚ V-chips in TVs ✚ Censor details of modus operandi 	25. Control Drugs & Alcohol <ul style="list-style-type: none"> ✚ Breathalysers in pubs ✚ Server intervention ✚ Alcohol-free events

According to the data presented in the table above, the rational choice perspective lends support to 25 different situational crime prevention techniques (for a more in-depth discussion of this framework, which has been modified and established since the 1980s, see Clarke, 2017). The concept of "target harden" is often all that is involved in crime prevention design, although it encompasses a wide range of strategies that may lessen the elements that contribute to the incidence of crime. These techniques have been demonstrated to be effective in reducing crime rates. problems all over the globe over the course of the last 35 years by changing the risks, benefits, efforts, justifications, and provocations that are associated with choices to offend.

3.6 Methodologies Plan



Figure 3.5 : Logo of R Project and RStudio

As has been mentioned, this thesis makes use of the Questionnaire Survey technique, which collects replies from several Malaysians via the use of Google Form. The R Project is a technique that should be used to analyse the findings of the study. This approach is widely used in a variety of fields, including educational research, market research, data mining, and many others. It can make predictions for a wide range of data for the purpose of classifying individuals and includes methods such as cluster analysis, factor analysis, and so on. In a nutshell, while working with RStudio simplifies R programming. An integrated development environment (IDE) for R is called RStudio, which means the R language powers RStudio. It has a console, a syntax highlighting editor that executes code directly, planning, history, debugging, and workspace management features. RStudio simplifies R communication for data science and statistics.

3.7 Potential Use of Validation Plan

As previously stated, there are twenty-five approaches for preventing crime that are grouped into five broad parts, each of which serves a distinct purpose in crime prevention activities. However, as mentioned in the crime triangle, each strategy has the same goal: to limit the probability and danger of crime, even if the offender is in one scope or near to the target. With such a reduction strategy, prospective offenders or potential perpetrators may be limited in some manner, either directly or indirectly.

Although SCP is primarily used as a concept for crime prevention in the physical world, it is also applicable as a measure for the prevention of cyber crime within the framework of the practise of cybersecurity. When applied to the realm of cyber crime, SCP measures centre their attention on limiting and or denying criminals opportunity to commit offences, as well as hindering their capacity to do so. Taking preventative actions against technical forms of cyber

crime is an example of situational crime prevention. Malware detection programmes, firewalls, which prevent unauthorised access by examining traffic and blocking traffic, and intrusion detection systems, which enable the tracking of cyberattacks as well as unauthorised access and use of systems, networks, data, services, and related resources are some examples of these technical measures.

SCP is concerned with the likelihood that cybersecurity attacks may materialise at some time. Consequently, these precautions are adopted since it is expected that dangers would materialise, necessitating corresponding response. While SCP focuses largely but still not completely on preventing crime, the truth is that even with these safeguards in place, criminal activity is likely to occur. As a result of this potential, cybersecurity incident detection, response, and recovery procedures are established.

CHAPTER 4

IMPLEMENTATION, RESULT AND DISCUSSION

4.1 Introduction

This chapter discusses the production of conducting surveys. The survey prepared to assess the effectiveness of Malaysians regarding cyber-attacks and the risk from the threat is still relatively low. After conducting a survey, some Malaysians randomly felt that hacking and data theft did not directly affect them. Thus, the relevant results were recorded for further justification.

4.2 Implementation Process

4.2.1 Research Objective

This study intends to to predict the criminology of cybercrime behaviour during pandemic covid - 19 in Malaysia by examine Malaysians' awareness in the following aspects,

- I. Student
- II. Parents / Adults
- III. Employee

4.2.2 Research Question

This investigation aims to provide a response to the following topic:

1. What is the present level of cybercrime behaviour in the criminology elements among Malaysians in COVID-19?

4.2.3 Findings of the study

The results of the research pertaining to demographics will be provided in the next section.

4.2.4 Demographic profile

There was a total of 142 persons from Malaysia included in this research, including 61 males and 81 females. The following figures depict personal information provided by these 142 respondents, including their age, race, state, status, and profession.

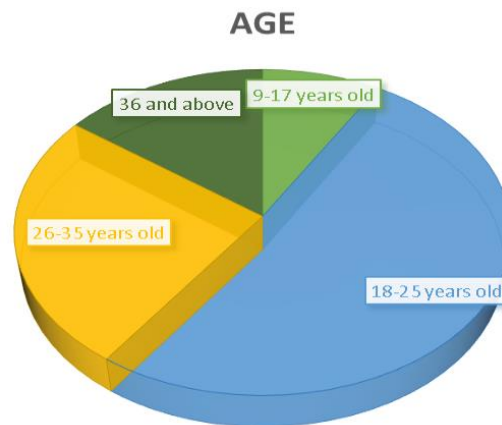


Figure 4.1 : Categorized of ages by the respondents

According to *Figure 4.1*, this is roughly the age that was considered for this survey on average. Teenagers between the ages of 18 and 25 make up as much as **78.90%** of the respondents to this poll. Adults between the ages of 26 and 35 make up **9.20%** of the respondents, while those aged 36 and beyond make up **8.5%**, meanwhile the percentage is only **3.50%** for the group of adolescents who are between the ages of 9 and 17 years old.

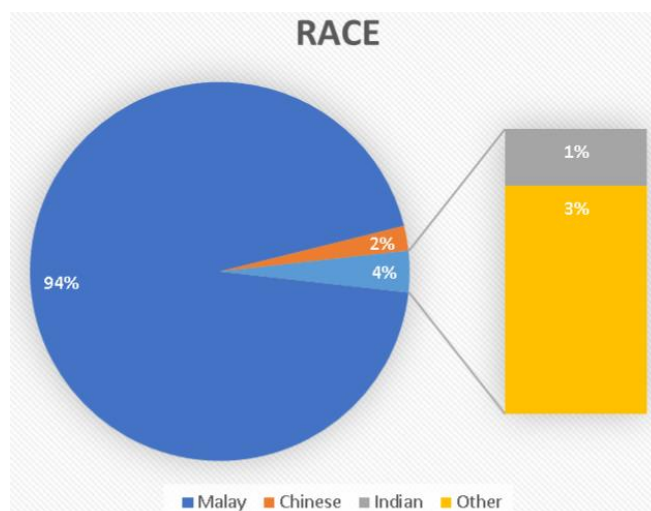


Figure 4.2 : Show the percentage of race in Malaysia based on respondents answer

As a result of the responses given by the respondents, the different racial groupings that may be found in Malaysia are shown in *Figure 4.2*. This poll was responded to by a total of **94.40%**

Malay people in Malaysia, followed by **4%** of people from other races, **3%** of Chinese people, and **1%** of Indian people.

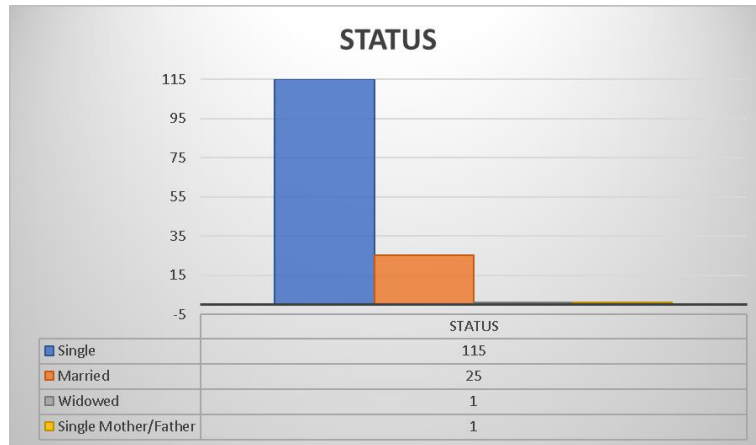


Figure 4.3 : Categorized of status by the respondents

Figure 4.3 depicts the status of 142 respondents, who have been characterized as having a single status **80.90%** of the time, a married status **17.70%** of the time, a widowed status **0.70%** of the time, and a single parent status **0.70%** of the time.

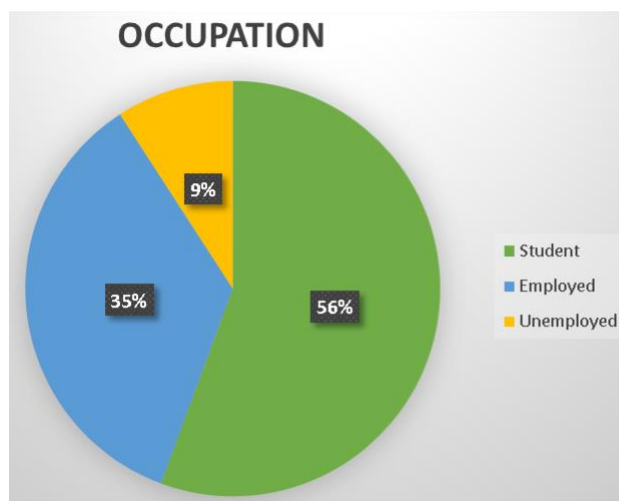


Figure 4.4 : Show the percentage of occupation respondents in Malaysia.

Figure 4.4 of the pie chart design that is shown above demonstrates that **56%** of the respondents are students. This is followed by **35%** of the respondents who work, and the remaining **9%** of respondents do not have jobs.

4.2.5 Parenting Observation

This part is geared specifically for married people, who will evaluate the capabilities of parents to monitor the online activities of their children as a form of both protection and prevention against cybercrime. This displays a statement regarding the efficacy of the response to determine the degree to which the parents agree with the assertion.

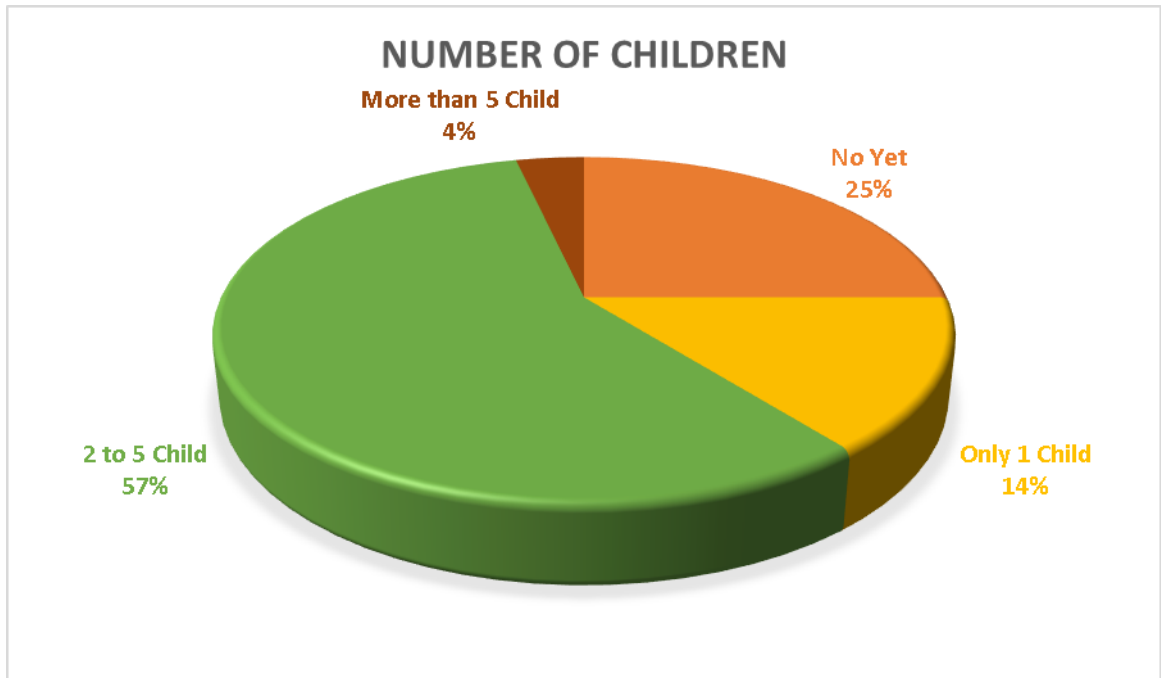


Figure 4.5 : Show the total number of children according to the married group respondent

Only **19.10%** of the 142 people who responded to the survey are married, as seen in *Figure 4.5*. According to the data, around one quarter of the respondents are married even though they are still raising their own children. There are only **25%** of respondents who are married but only have one kid. This is followed by **57.10%** of respondents who have between 2 and 5 children, and only **3.60%** of respondents have more than 5 children.

Table 4.1 : Shows how vigilant parents monitor the technology that being used by their kids.

No	Item	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Very Disagree (%)
P1	Limited the amount of time their spend on gadget	5.60	1.68	0.56	-	-
P2	Checked the browser history to see which sites they visited	4.20	2.80	0.84	-	-
P3	Do you know your children's online passwords	3.08	1.68	2.80	0.28	-
P4	Do you use internet filtering software on all devices your child has access to	2.52	2.52	1.68	-	-
P5	Do you have an online rules agreement with your child	3.64	2.24	1.40	0.56	-
P6	Do you know how many hours a week your child spends chatting online with others	2.52	1.96	3.36	-	-
P7	Is the devices your child uses kept in a high traffic area in your home	1.40	3.08	3.36	-	-
P8	Do you allow your child to download any game apps	1.68	1.96	3.08	0.56	0.56
P9	Does your child know of the safety tips	2.52	2.52	2.52	0.28	-

Table 4.1 demonstrates that some parents continue to neglect their children in items **P5**, **P8**, and **P9**. Parents should establish limits on their children's internet usage while they are still in school in order to keep them from getting hooked on it. However, **0.56%** of parents do not set these limits, and **1.40%** of parents are "Neutral" about it. In response to question **P8**, **3.94%** of parents claimed they were okay with their kids' downloading games, while **3.08%** of parents chose "Neutral." Due to this, players may encounter gaming applications that need transactions without recognizing it. Regarding question **P9**, **0.28%** of parents said their kids were unaware of safety precautions, whereas **2.52%** of parents gave "Neutral" as their answer. To stop the

incidence of cybercrimes, parents must stop their kids from "*strike the iron while it's hot*" beginnings.

4.2.6 Cyber crime Experience

This part was developed so that an assessment may be made about the level of respondent comprehension with respect to cybercrime.

Table 4.2: Show basic information from respondents.

No	Item	Yes (%)	Maybe (%)	No (%)
C1	Do you have prior knowledge about criminology?	32.40	35.20	32.40
C2	Do you have any experience in cyber-crime?	41.50	17.60	40.80
C3	Do you have antivirus software installed on your PC/Mac?	62.00	18.30	19.70

The data provided by the respondents, as shown in *Table 4.2* above, is relatively inadequate, notably for item **C1**. Only **32.40%** of respondents are aware of the criminology that is taking place in the surrounding area, while **32.40%** are unaware of it and **35.20%** are unsure. In response to question **C2**, **41.50%** of respondents said that they have been a victim of cyber crime at some point in their lives. **62.00%** of respondents were able to successfully install antivirus software on their computers, indicating that they are aware of the possibility that their computers may be infected with computer viruses.

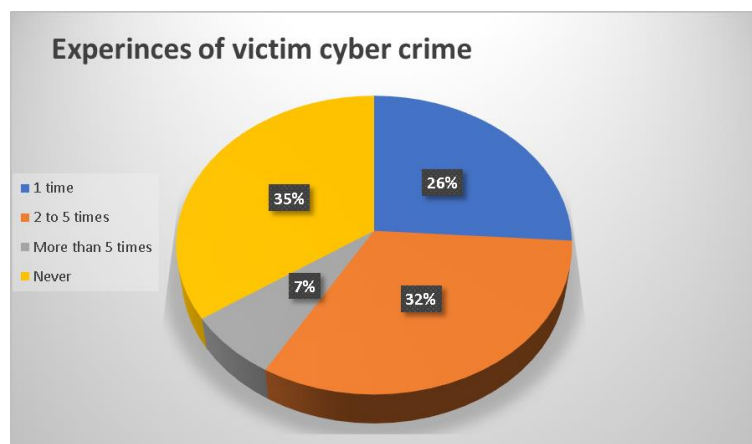


Figure 4.6 : Show the number of experienced being a victim by respondents

According to the poll that was carried out, **35%** of the people who responded had never been a victim of any kind of cyber crime. Only **26%** of respondents have ever been victims of

cybercrime, whereas **32%** of respondents have been victims of cyber crime anywhere from two to five times. In addition, seven percent of those who responded said that they had been the target of cyber crime more than five times.

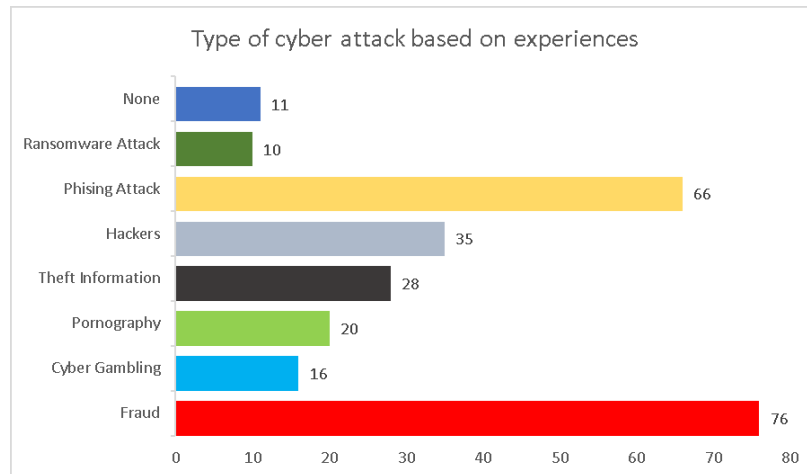


Figure 4.7 : Show the experiences of cyber-crime by respondents

According to *Figure 4.7*, the sort of cyber crime that the respondent encountered the most often was fraud, which accounted for **53.52%**, followed by phishing attacks, which accounted for **46.48%**. Only **24.65%** of all crimes committed are considered hacking, **19.72%** are considered information theft, and **14.08%** are considered pornographic. While **11.27%** of respondents believe that cyber gambling is the least serious offence, **7.04%** believe that ransomware attacks are the most serious. Surprisingly, **7.75%** of respondents had never been the victim of any kind of cyber-criminal incident.

Table 4.3: Show respondent’s experiences online.

No	Item	Yes (%)	Prefer Not to Answer (%)	No (%)
E1	I've been cyberbullied victim	51.12	4.26	146.26
E2	I've cyberbullied someone else	11.36	5.68	184.60
E3	Someone else has pretended to me online.	52.54	-	149.10
E4	Someone has sent/share me messages with sexual content.	73.84	-	126.38
E5	I've been the victim of fraud online and lost money.	15.46	-	154.78

Due to the obvious responses provided by the respondents themselves, *Table 4.3* illustrates how hazardous this cybercrime is. **51.12%** of respondents have reported having experienced cyberbullying, according to item **E1**. If this keeps happening, the responder can experience any emotional or bodily discomfort. While **11.36%** of respondents to Item **E2** acknowledged that they have cyberbullied someone else despite knowing it was unethical to do so. **9.94%** of respondents also declined to answer to remain anonymous for Item **E1** and **E2**. Additionally, **52.54%** of respondents acknowledged that they had been impersonated by other users online. Due to this, they may become the victim of fraud and other forms of victimization. In addition, **73.84%** of responders to question **E4** acknowledged receiving sexually explicit communications. Then, Item **E5** demonstrates that some respondents continue to lose money while engaging in online activities because of believing or accepting threats from cybercriminals.

4.2.7 Threat Severity Cyber crime

In the following paragraphs, we will discuss the likelihood of an individual being a victim of cyber crime.

Table 4.4: Show the statement about threat vulnerability of respondents.

No	Item	Very Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Very Disagree (%)
T1	Have you ever heard of someone being a victim of cybercrime	93.72	83.78	118.46	-	4.26
T2	Have you ever been hacked through email, social net or blogs	26.98	39.76	55.38	12.78	29.82
T3	Do you allow others (Friends, relatives) to use your personal ID.	5.68	28.40	51.12	15.62	73.84
T4	Have you seen anything on the news about people being harassed online	96.56	73.84	22.72	-	4.26
T5	Have you found someone using your photo, profile, bank detail (In social network) or duplicating your personal details	19.88	19.88	48.28	12.78	-

T6	If you have found someone using your photo, profile, bank detail, did you report to admin website	107.92	44.02	31.24	1.42	4.26
T7	Do you feel safe about your information when you online	11.36	25.56	62.48	18.48	63.90
T8	Have you ever lost money due to cyber crime	28.40	25.56	35.50	12.78	65.32
T9	Do you think that the laws in effect are able to control cyber criminal	85.20	48.28	42.60	1.42	11.36

Table 4.4 shows statements about threat vulnerability that have been answered by unsatisfactory respondents such as in **T3**, **T7** and **T8**. As shown that as many as **177.50%** of respondents took the issue of falling prey to cyber crime, **T1**. In **T3**, there are still **34.08%** of respondents agreeing to allow other people to use personal IDs while theft is easy to do if it applies. **T7** said that is there any security of details when online, **36.92%** of respondents agreed saying it is safe if their information is protected by Data Protection and Data Security (**DPDS**). For **T8** as well, **53.96%** of respondents said they fell prey to money-losing scams due to this cyber crime that still needs to be contained.

4.2.8 Self-Efficacy

This section explains how a respondent's capability to take precautions with their own equipment relates to the process of taking preventative steps online as well as the comfort level associated with doing so. This is the situation, and every one of the findings is the view of the responder to agree with the assertion about self-efficacy.

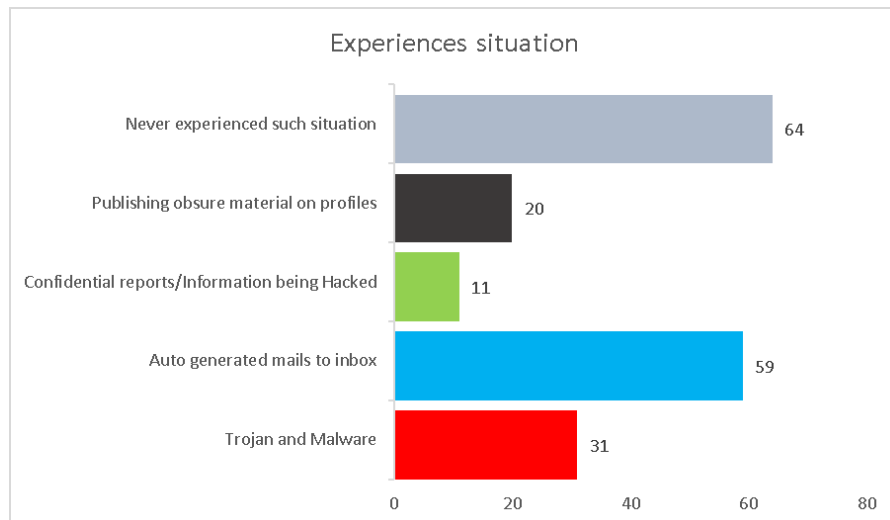


Figure 4.8 : Show the situation of experiences by respondents

The lived of respondent experiences are shown in *Figure 4.8* as they relate to various situations. According to the circumstances, the percentage of respondents who are getting automatically produced emails in their inboxes is greatest at **41.55%**. The second problem is that **21.83%** of respondents have been infected with malware and trojans. This is followed by the publication of cryptic content on profiles by **14.08%** of respondents, and **7.75%** of respondents have had their sensitive reports and information stolen. A little less than half of those who responded had never been in such a dilemma.

Table 4.5: Show the rating of how good respondents protect their devices.

No	Item	Very Good (%)	Good (%)	Ok (%)	Poor (%)	Very Poor (%)
S1	Use strong password by using combination of all.	124.96	62.48	14.20	-	-
S2	Secure computer by activating the firewall and use anti-virus/malware software.	102.24	65.32	28.40	4.26	1.42
S3	Block Spyware attacks.	90.88	61.06	46.86	1.42	1.42
S4	Secure mobile devices.	102.24	72.42	26.98	-	-
S5	Install the latest operating system and software updates.	100.82	71.00	25.56	4.26	-
S6	Protect data by using encryption sensitive files.	92.30	61.06	46.86	1.42	-
S7	Review bank and credit card statements regularly.	113.60	52.54	28.40	4.26	2.84
S8	Secure wireless network.	93.72	72.42	31.24	1.42	2.84

The results for device of respondent patient care are shown in *Table 4.5*. Items **S2**, **S3**, **S7**, and **S8** do not provide sufficient outcomes when it comes to recommended practices for utilizing gadgets. A quarter of the people who responded to the study said they did not use anti-virus and firewall software to protect their computer. This is accurate; **153.33%** of respondents use sensitive files to encrypt their data to protect it from viruses. Additionally, **2.84%** of respondents do a bad job of protecting malware against attacks. In addition, **7.10%** of respondents do not routinely monitor their bank and credit card bills, even though **124.96%** do so. As a result, if it occurs, it will be impossible to tell the difference between a money withdrawal and receipt. Even **4.26%** of those surveyed failed to set up a secure wireless network, which might result in wireless network line theft.

Table 4.6: Cyber crime behavior of participants in online fraud concerns

No	Item	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly Disagree (%)
F1	Created a trustworthy online friendship with strangers	34.08	39.76	65.32	32.66	29.82
F2	Ignored emails from reputable organizations with odd or excellent news	72.42	62.48	48.28	4.26	12.78
F3	Respond to SMS messages advertising competitions offering significant prizes.	26.98	18.46	36.92	35.50	83.78
F4	Never rely on strangers' online identity disclosures	119.28	44.02	24.14	7.10	7.10
F5	Never think about paying any money for services provided by an internet website.	102.24	44.02	38.34	11.36	4.26
F6	Willing to agree with internet pals' requests to deposit money.	21.30	11.36	44.02	35.50	89.46
F7	Aware of and capable of spotting the most recent internet frauds	69.58	71.00	52.54	1.42	7.10
F8	Accept strangers' photos on the Internet.	21.30	22.72	53.96	32.66	71.00
F9	Wouldn't hesitate to meet up with online pals in person.	28.40	21.30	56.80	21.30	73.84

There were unfavorable answers to four issues about online fraud. **F6**, **32.66%** of respondents were willing to provide online friends deposit money, while **44.02%** of respondents selected “Neutral”. Only **25%** of respondents agreed with the statement for item **F7**, “*understanding and capacity to spot the current online scam*,” while **52.54%** of respondents said they were “Neutral” about the topic, with **8.52%** of respondents choosing to disagree. Although **53.96%** of **F8** respondents claimed to be “Neutral”, researchers were perplexed given that **103.66%** of respondents said they did not trust images of strangers posted online. In **F9**, **49.70%** of respondents said they would be open to making acquaintances online, while **95.14 %** said they were against it.

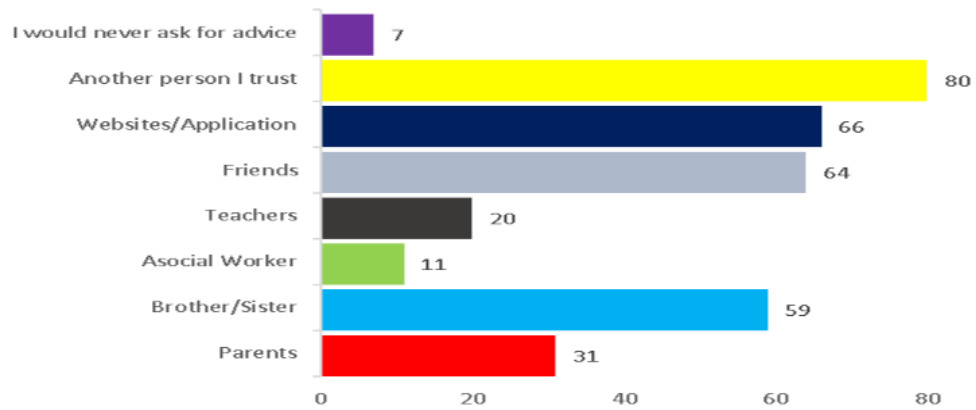


Figure 4.9 : Show the rating how respondents get advice about staying online

Number of times respondents provide their thoughts or seek assistance from others with greater expertise when it comes to issues with the internet. According to *Figure 4.9*, most respondents go to trusted friends and family members for guidance first, followed by websites and apps that they can research on their own. There are also individuals who will seek the guidance of friends who are more knowledgeable, particularly those who work in the area of information technology. A total of **59** respondents said that they would like to get advice from the person who is physically nearest to them, such as a brother or sister, while **31** respondents indicated that they would prefer to get advice from their parents. As a result, 31 of the respondents received exposure from their professors, while **11** of the respondent's received exposure from their social workers. In addition, seven of the individuals who participated in the survey made the decision not to seek guidance from anybody, which increases the likelihood that they may encounter issues when using the internet.

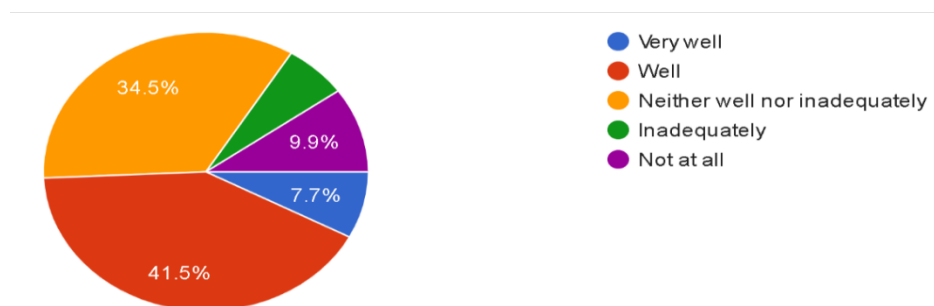


Figure 4.10 : Show the school prepared for dealing with cyber threat

Figure 4.10 shows that over half of the respondents had early experience managing cyber issues, which is beneficial for academic success. However, **34.50%** of respondents think that the exposure they get in school may not be enough to fulfil their expectations. **9.90%** of respondents reported receiving no instruction about how to prepare for dealing with cyber issues, while **6.40%**

of respondents felt unable to cope with cyber hazards they had been exposed to at school. Therefore, if early whistleblowers are not provided, there are still plenty of responders who will have expertise with cyber crime.

4.3 Testing and Result Discussion

In this part are where all methods that have been introduced in chapter 3 will be implemented and test the process by the R Project Software using RStudio. The testing result shows the success of the experiment that has been testing. The result will be different because it depends on responder answer.

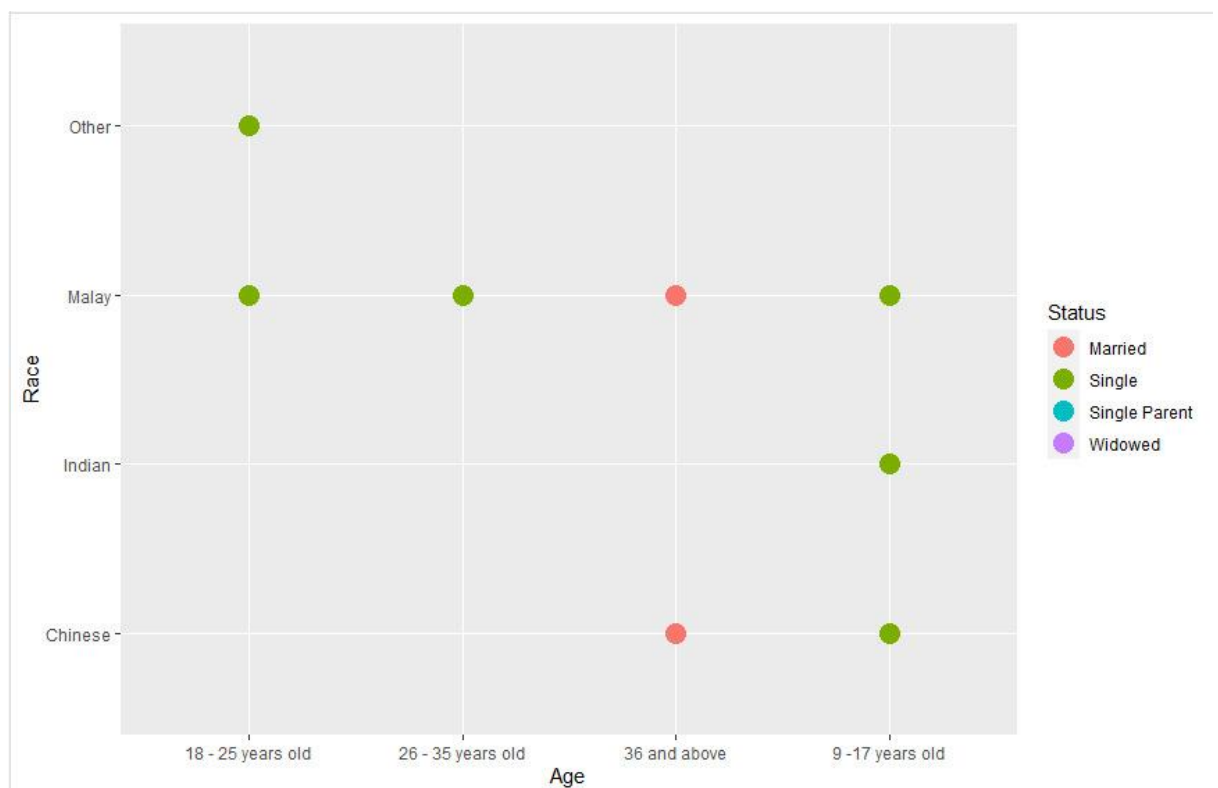


Figure 4.11 : Show the result of respondent detail.

The figure above shows the result of the process in RStudio software. In *Figure 4.11* demonstrates that those respondents classified as being in the childhood and teenage age ranges are more likely to have a status of single, while those respondents classified as being in the adult age range are more likely to have a status of married.

4.3.1 Trial of testing for parent observation

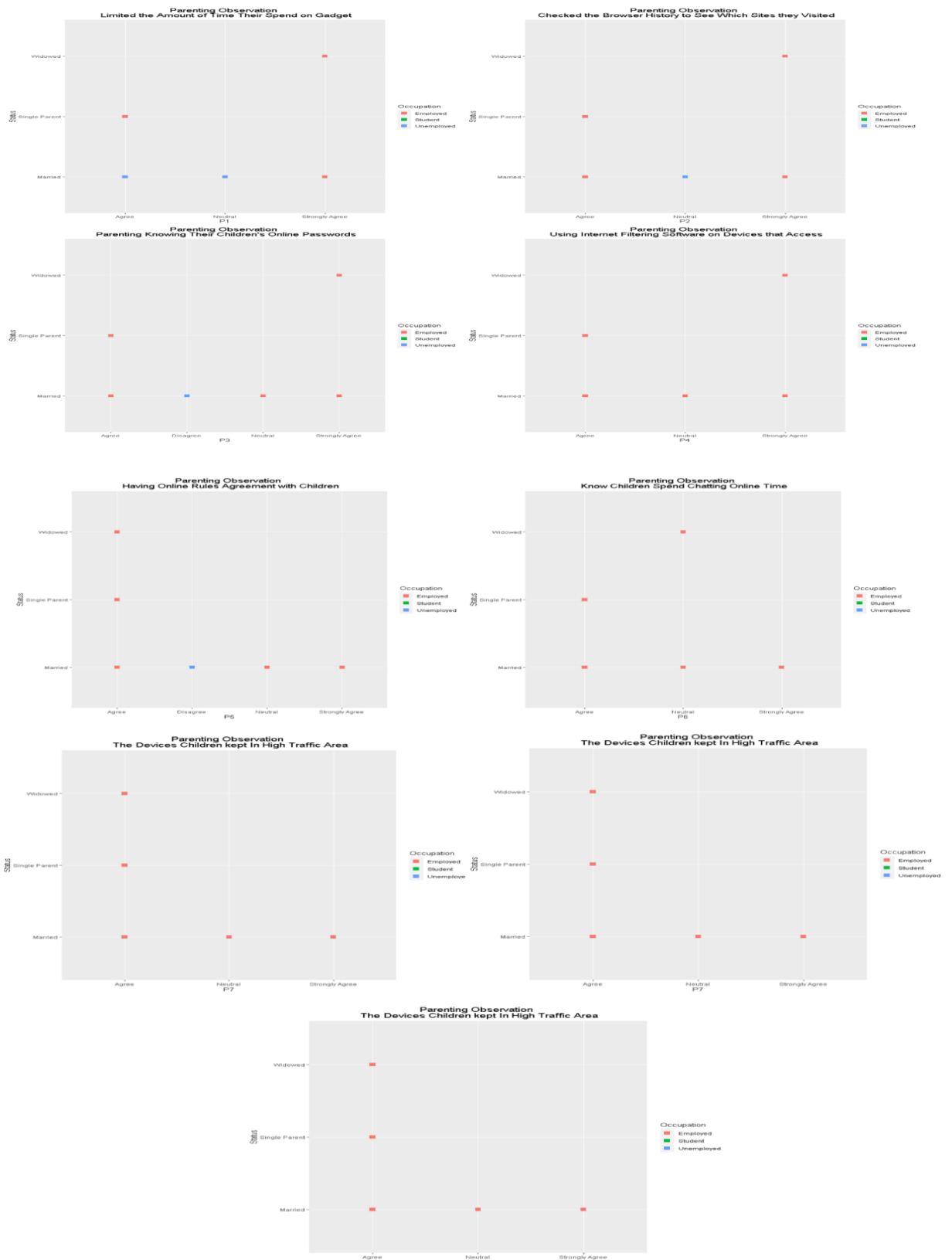


Figure 4.12 : Result based on parent observation

As can be seen in *Figure 4.12*, a significant portion of the respondents who are married already have careers of their own. This demonstrates that working parents are more aware of their

surroundings and make every effort to prevent their children from being involved in undesirable behaviours by always monitoring their whereabouts and activities.

4.3.2 Trial of testing for cybercrime experience

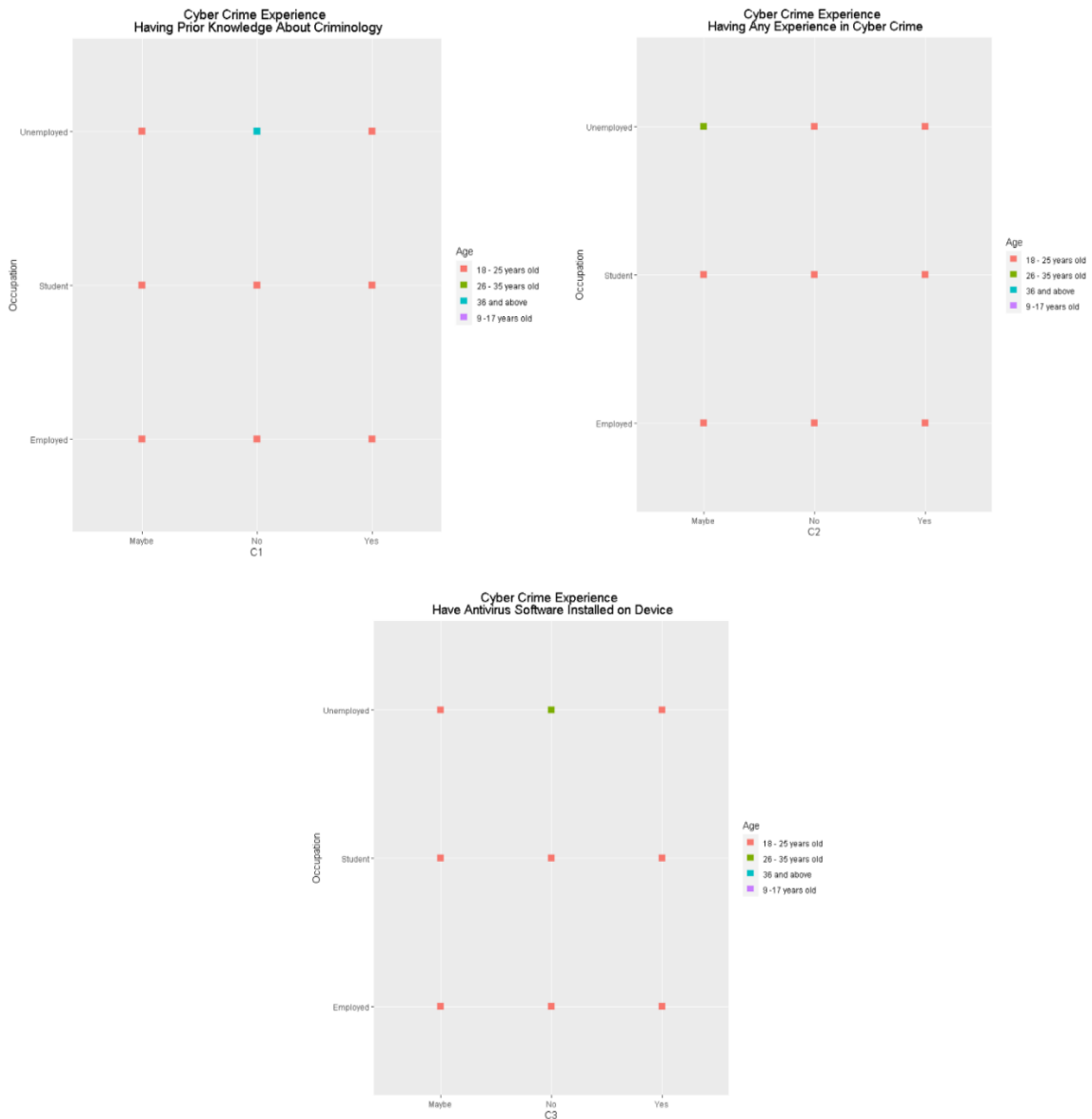


Figure 4.13 : First trial testing of cyber crime experience

Figure 4.13 demonstrates that there are a greater number of teens who are employed while also attending school. In addition, half of the respondents are aware of the actions associated with criminology, while the other half of the respondents are still in the process of becoming familiar with cyber crime.

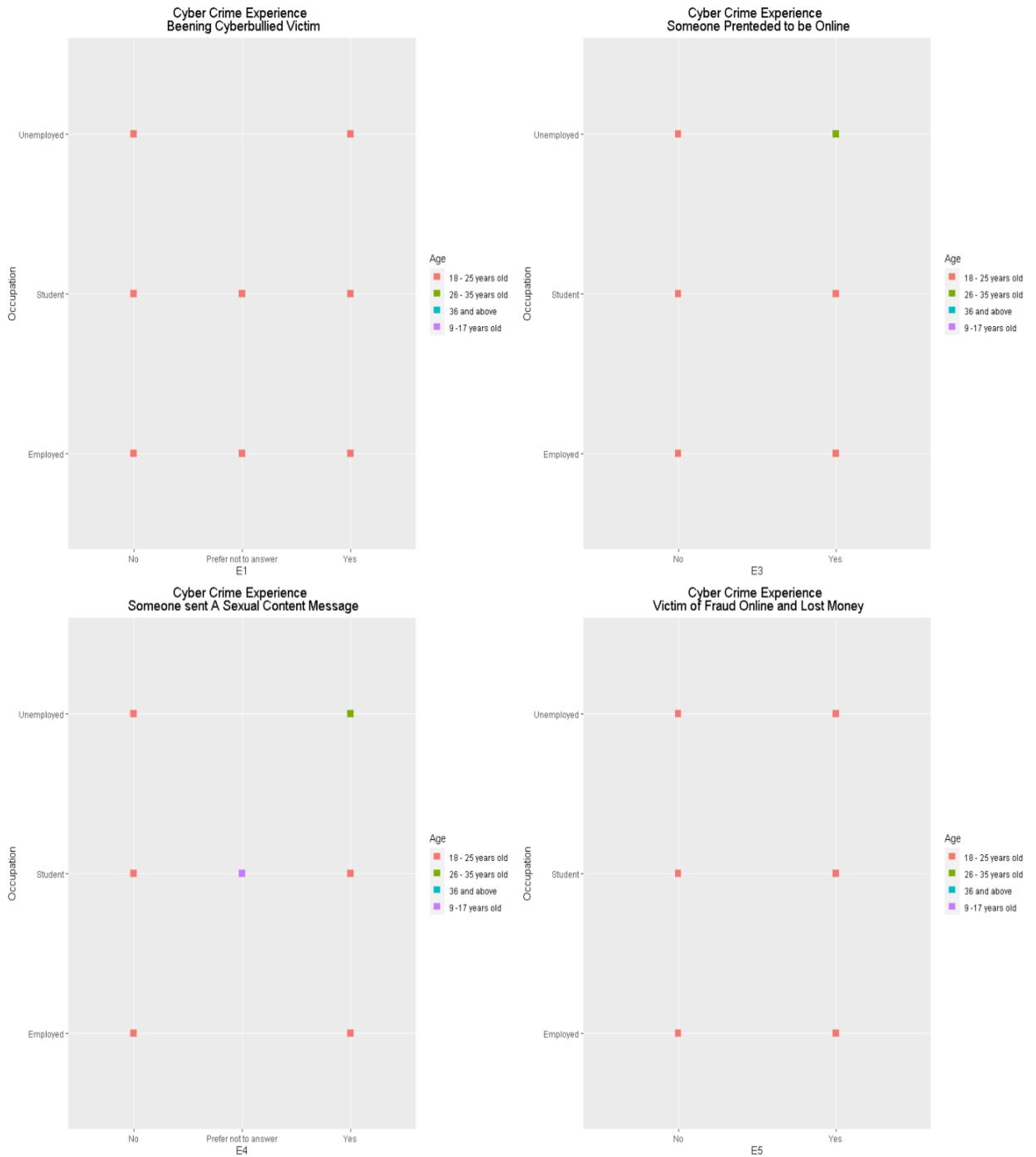


Figure 4.14 : Second Trial of cyber crime experiences

As shown in *Figure 4.14*, respondents aged 18 to 25 who are in school, working, or not working all gave a negative response to the question of whether they have expertise regulating cyber crime while online.

4.3.3 Trial of testing for threat severity cyber crime

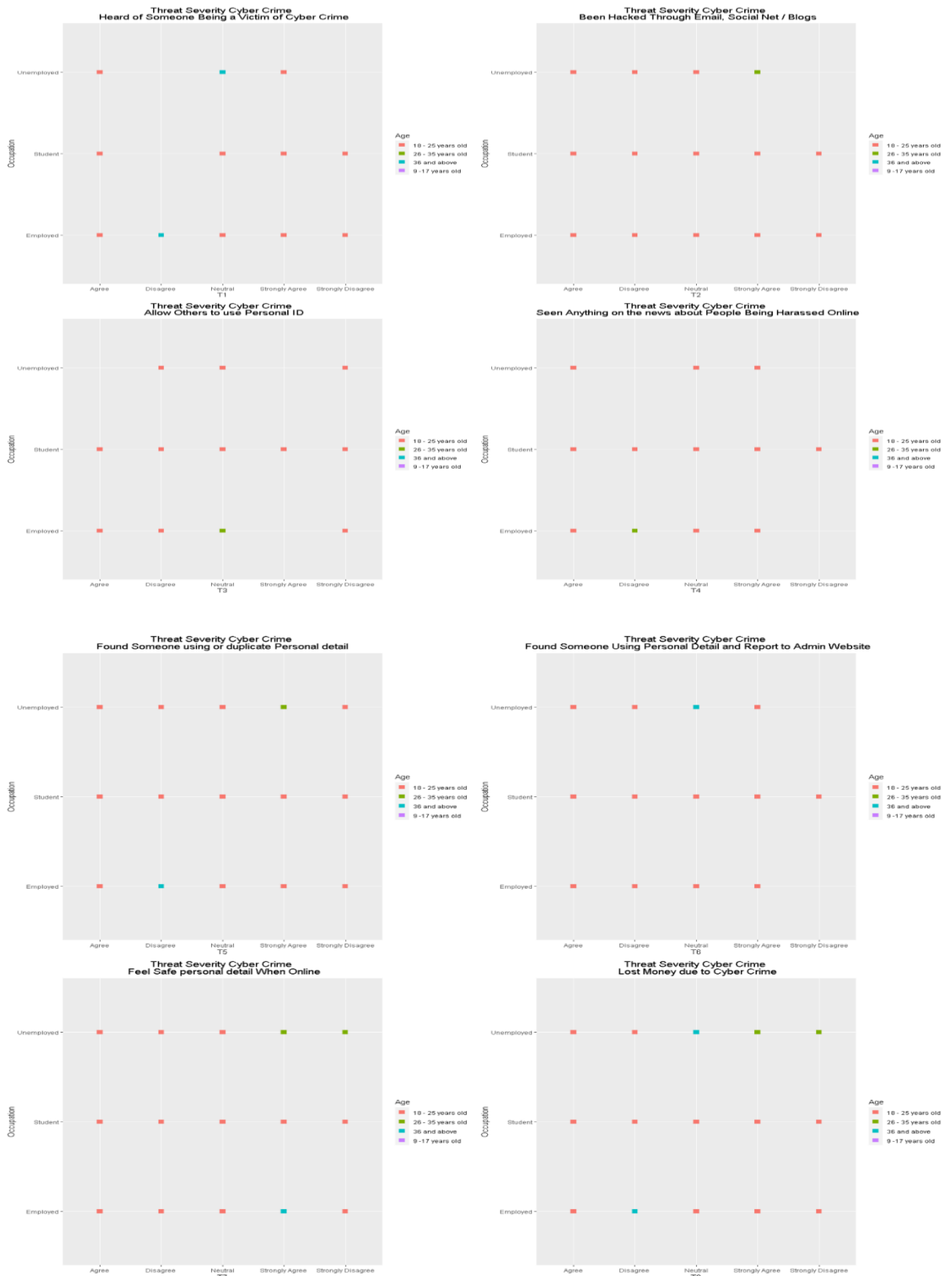


Figure 4.15 : Result of trial testing for threat severity cyber crime

The findings that were published are shown in *Figure 4.15* according to the severity of the cybercrime threat. Considering this, the conclusion that teens should be prioritised has not

changed; in this instance, the result shown that respondents picked all of the available response categories.

4.3.4 Trial of Test for Self- Efficacy

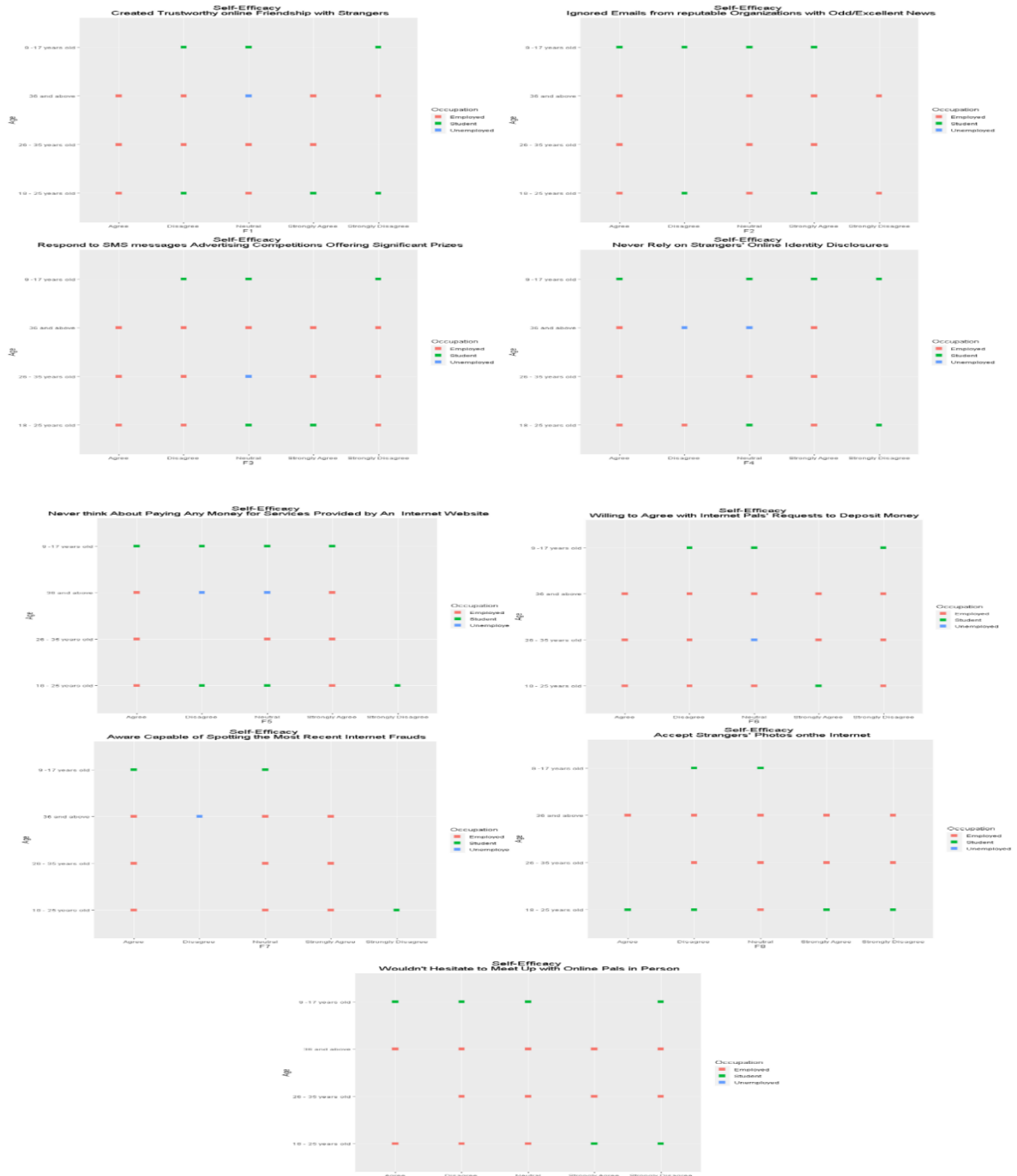


Figure 4.16 : First trial testing for self-efficacy.

The findings that have been provided in terms of self-efficacy on the way in which respondents maintain their gadgets are shown in *Figure 4.16*. This result demonstrates that each responder

plays a part in protecting the devices they own from being vulnerable to the attacks of cybercriminals.

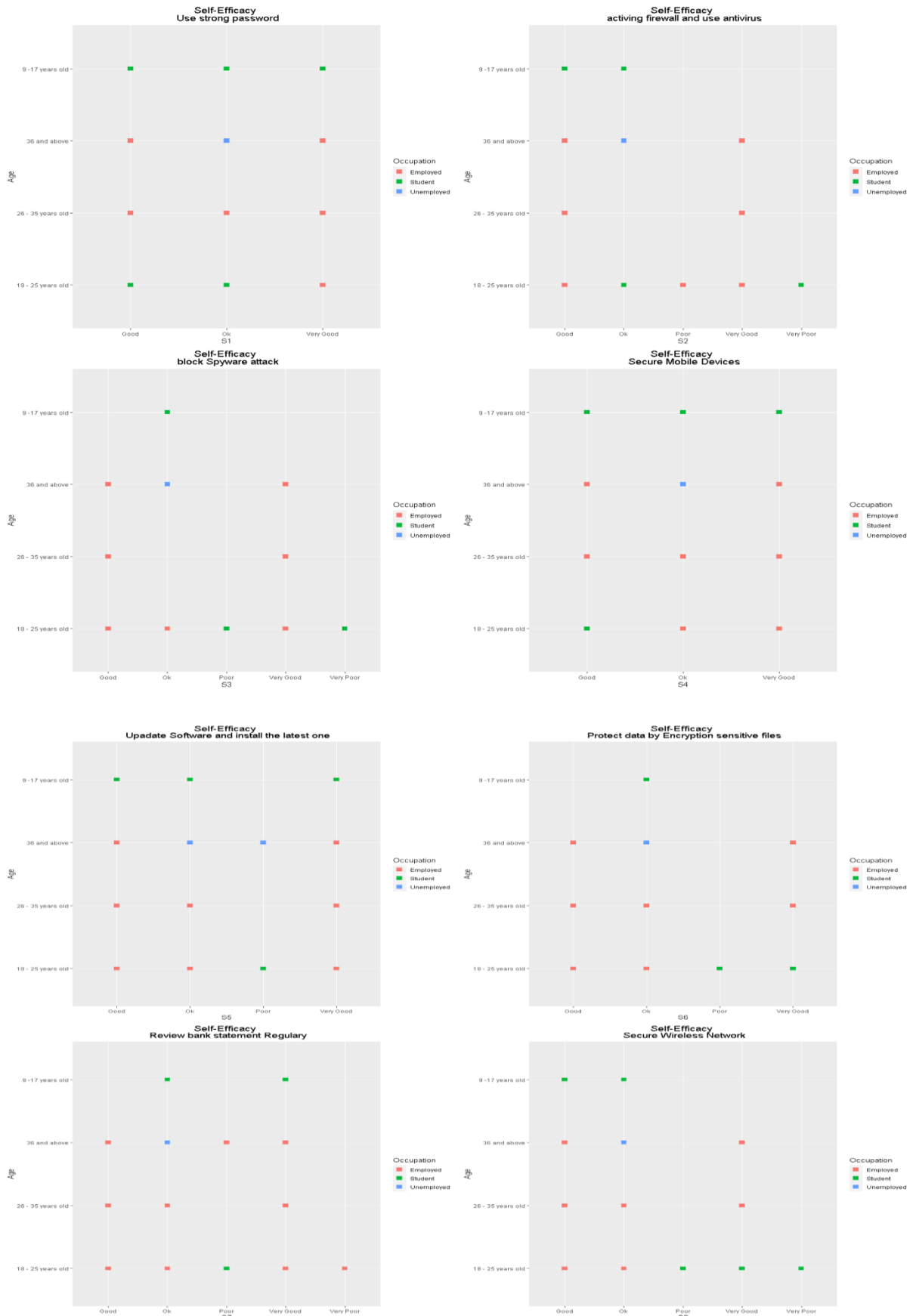


Figure 4.17 : Second trial testing for self-efficacy

The findings that have been provided in terms of respondents' self-efficacy on their awareness of online fraud are shown in *Figure 4.17*. This result demonstrates that all of the respondents still need a significant amount of details on this online scam. This is since the results shown in the diagram reveal that practically all of the respondents provided responses that were either Good or Ok.

CHAPTER 5

CONCLUSION

5.1 Introduction

This chapter is going to provide a summary of the study project. By using the idea of situational crime prevention, this study has been successful in accomplishing the goals that were outlined in the previous section Situational Crime Prevention (SCP). According to the findings of the study, most incidents that take place are attributable to SCP. In addition, in **section 5.2**, a more in-depth summary of the benefits and drawbacks of utilising R Project Software to analyse respondent data will be provided, and then, in **section 5.3**, an explanation of the study that will be carried out in the subsequent section will be provided.

5.2 Research Constraint

According to this research, obtaining responses from people located throughout Malaysia is somewhat challenging. This is because some Malaysians do not enjoy responding to surveys, and another group of people are still unable to use modern technology. This is especially true of veteran citizens and children who are still enrolled in school. In addition, the timeframe to learn the new RStudio programme is insufficient since it has been used to finish the data visualisation for this survey and also the problem when downloading this software. For this RStudio Software, may download this programme from several different websites, but the vast majority of them demand to pay, so in order to discover a website that does not charge students, because need to create a lot of referrals from YouTube. In conjunction to that, being able to learn something new and exerting a significant amount of effort to do so may both add to one's knowledge.

5.3 Future Work

There are several suggestions that can be executed for future improvements of this research. The government needs to sensitize and create campaigns on early prevention of becoming a cybercriminal or victim from school to work. This is the case because, according to the research, a greater number of respondents preferred to obtain any advise from family and teachers rather than performing any searches on the web or internet, even though we live in an era when everything is at our fingertips.

Provides many antiviruses that are easy to install and free. Since many antivirus programmes, like McAfee, SMADV, and others, demand an extremely high payment in order to make use of all of the capabilities that are offered. Therefore, to protect students and staff from falling victim to cybercrime, educational institutions and government authorities should make antivirus programmes freely available to them.

5.4 References

- [1] Bernam.com. (Sept, 2021). *STATISTIK COVID-19 DALAM MALAYSIA*.
<https://www.bernama.com/misc/covid-19/index.php>
- [2] Bernam.com. (Jan 12, 2021). *Agung Isytihar Darurat Bendung COVID-19 di Malaysia*.
https://www.bernama.com/bm/am/news_covid-19.php?id=1920898
- [3] DOSM. (Nov 25, 2021) - *PRESS RELEASE CRIME STATISTICS PUBLICATION 2021*.
<https://www.dosm.gov.my/v1/index.php?r=column/pdfPrev&id=eHE0eGZWSmNROG1BbHR2TzFvZzZxQT09>
- [4] “Review of the Roots of Youth Violence: Literarure Reviews.” Chapter 3 : Rational Choice And Routine Activities Theory. N.p., n.d. Web. 14 Apr. 2014.
<https://www.youtube.com/watch?v=lWcLmzbB4kM>
- [5] Chandrasehkar M.(June 2005) – *Differences In Pattern of Violent Crimes Between Illegal Immigrants and Malaysians*.
<http://eprints.usm.my/46660/1/Chandrasehkar%20Muthu.pdf>
- [6] Farahah R, W. Shahrazad., & M. Rahim K. (Nov 25, 2019). *FEAR OF CRIMES AMONG UNIVERSITY STUDENTS IN MALAYSIA: ANAYSES OF CONTRIBUTING FACTORS*. [http://web.usm.my/km/37\(2\)2019/km37022019_7.pdf](http://web.usm.my/km/37(2)2019/km37022019_7.pdf)
- [7] CANADIAN BANKERS ASSOCIATION. (Sept 22, 2021) – *Cyber security & fraud prevention learning guide*. <https://cba.ca/fraud-prevention-101>
- [8] ResearchGate. Narayanaswamy V.R., & Harinarayana N.S. (Jan 2016). *ONLINE SURVEY TOOLS: GOOGLE FORM*.
https://www.researchgate.net/publication/326831738_Online_survey_tools_A_case_study_of_Google_Forms
- [9] PJEE. Sari., Iswahyuni., Rejeki., & Sutanto. (Oct 28, 2020). - *GOOGLE FORMS AS AN ELF ASSESSMENT TOOL*.
https://ojs.fkip.ummetro.ac.id/index.php/english/article/viewFile/3037/pdf_1
- [10] DCU. (June, 2020). – *DCU DATA PROTECTION GUIDANCE: GOOGLE FORM*.
<https://www.dcu.ie/sites/default/files/inline-files/google-forms-guidance-v1.pdf>
- [11] ResearchGate. Saidatulakmal M., Abdelhak S., Thurai M. N., & S. Rohaya M.R. (Aug, 2016) – *CYBERCRIME AMONG MALAYSIA YOUTH*.

https://www.researchgate.net/publication/334824052_Cybercrime_among_Malaysian_Youth

[12] ResearchGate. Kyung S.C., & Claire L. (Aug, 2018). – THE PRESENT AND FUTURE OF CYBERCRIME, CYBERTERRORISM AND CYBERSECURITY.

https://www.researchgate.net/publication/328433593_The_Present_and_Future_of_Cybercrime_Cyberterrorism_and_Cybersecurity

[13] Kaggle. Shirshir. (2017). – *CYBER CRIME*.

<https://www.kaggle.com/datasets/shisnir/cyber-crime>

[14] Kaggle. Daylight Security Research Lab. (2019). – CYBERSECURITY IMAGERY DATASET. <https://www.kaggle.com/datasets/daylight-lab/cybersecurity-imagery-dataset>

[15] College of Policing. (n.d.). – *WHAT IS SITUATIONAL CRIME PREVENTION?*

<https://www.college.police.uk/guidance/neighbourhood-crime/what-situational-crime-prevention>

[16] ResearchGate. (n.d.). – *THE 25 TECHNIQUES OF SITUATIONAL CRIME PREVENTION WITH CRIME PREVENTION TECHNIQUES*. https://www.researchgate.net/figure/The-25-techniques-of-situational-crime-prevention-with-crime-prevention-examples-of-each_tbl1_319715258

[17] UNODC. (n.d.). – *E4J UNIVERSITY MODULE SERIES : CYBERCRIME – MODULE 9 : CYBERSECURITY AND CYBERCRIME PREVENTION – PRACTICAL APPLICATIONS AND MEASURES*./ United Nations Office on Drugs and Crime. <https://www.unodc.org/e4j/zh/cybercrime/module-9/key-issues/situational-crime-prevention.html>

[18] SINARHARIAN | T. Buqhairah T. M. A.. (June 28, 2021) – *4,327 KES JENAYAH SIBER LIBAT KERUGIAN RM77 JUTA DILAPORKAN*. <https://www.sinarharian.com.my/article/146770/BERITA/Nasional/4327-kes-jenayah-siber-libat-kerugian-RM77-juta-dilaporkan>

[19] WISER| Ariffmac. (Nov 23, 2020). – *INSIDEN JENAYAH SIBER DI MALAYSIA BAGI TAHUN 2020 MENINGKAT BERBANDING 2019*. <https://wiser.my/insiden-jenayah-siber-di-malaysia-bagi-tahun-2020-meningkat-berbanding-2019>

5.5 Appendix

5.5.1 Gantt Chart

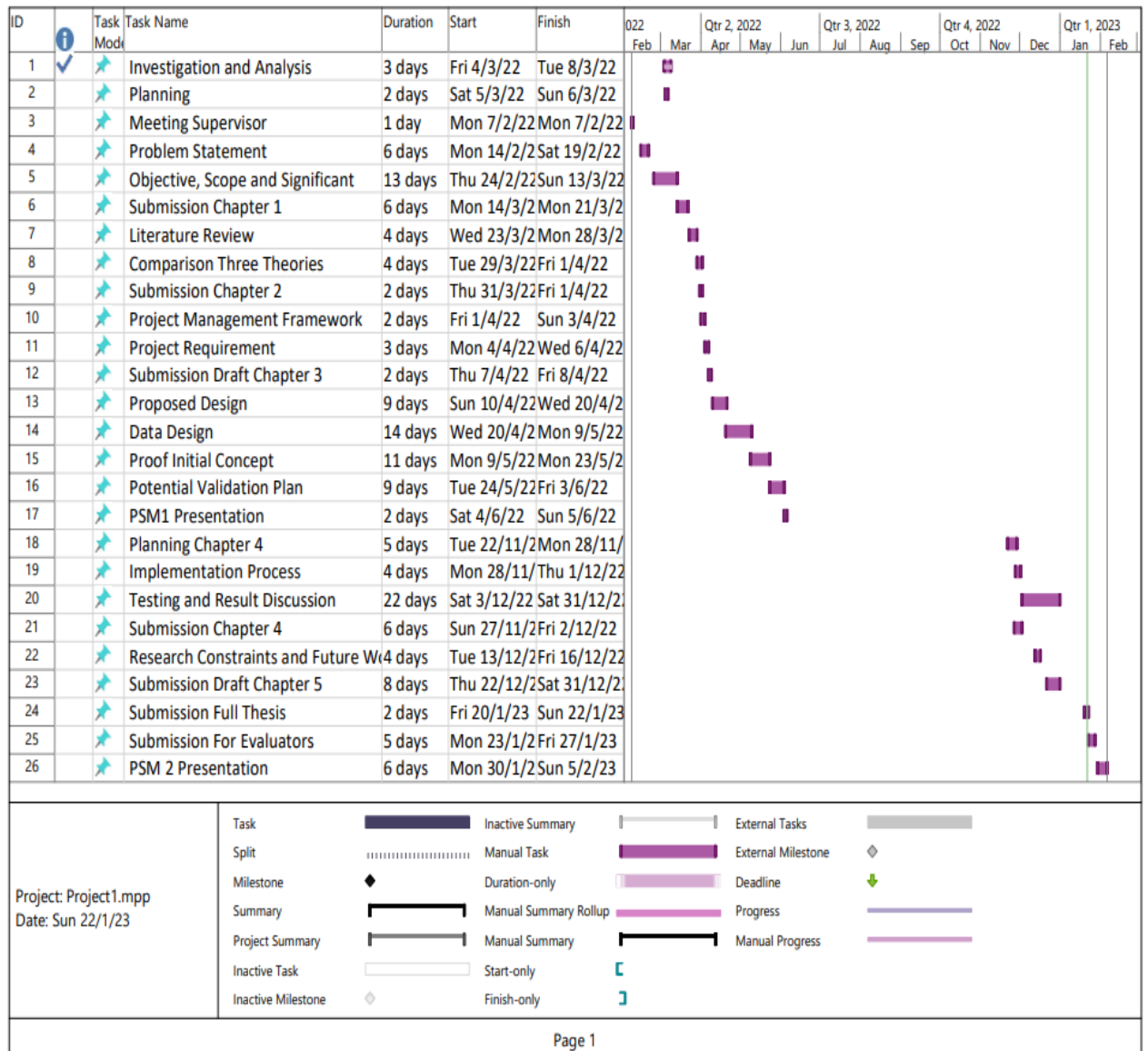


Figure 5.1 : The process of PSM

5.5.2 Information Data of Output RStudio

```

> PO<- read_csv("Parentobserve.csv")
Rows: 27 Columns: 12
-- Column specification -----
Delimiter: ","
chr (12): status, occupation, Num_Child, P1, P2, P3, P4, P5, P6, P...

i Use `spec()` to retrieve the full column specification for this data.
i Specify the column types or set `show_col_types = FALSE` to quiet this message.
> summary(PO)
  status      occupation      Num_Child
Length:27    Length:27      Length:27
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
  P1      P2      P3
Length:27 Length:27    Length:27
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
  P4      P5      P6
Length:27 Length:27    Length:27
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
  P7      P8      P9
Length:27 Length:27    Length:27
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
> view(PO)

```

Figure 5.2 : Summary Coding for Parenting Observation

	Status	Occupation	Num_Child	P1	P2	P3	P4	P5	P6	P7	P8	P9
1	Married	Employed	2-5 child	Agree	Agree	Agree	Neutral	Neutral	Neutral	Neutral	Agree	Agree
2	Married	Employed	1 only child	Agree	Neutral	Agree	Agree	Neutral	Neutral	Neutral	Strongly Agree	Neutral
3	Married	Employed	No child yet	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Agree	Neutral	Neutral
4	Married	Employed	No child yet	Strongly Agree	Strongly Agree	Neutral	Neutral	Strongly Agree	Strongly Agree	Neutral	Neutral	Neutral
5	Married	Employed	2-5 child	Agree	Agree	Agree	Agree	Agree	Agree	Agree	Neutral	Agree
6	Married	Unemployed	1 only child	Strongly Agree	Agree	Disagree	Agree	Disagree	Neutral	Agree	Very Disagree	Disagree
7	Married	Unemployed	2-5 child	Strongly Agree	Agree	Neutral	Agree	Disagree	Neutral	Neutral	Neutral	Neutral
8	Married	Unemployed	2-5 child	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Agree	Neutral	Agree
9	Married	Employed	more than 5 child	Strongly Agree	Strongly Agree	Neutral	Strongly Agree	Neutral	Agree	Strongly Agree	Agree	Neutral
10	Married	Employed	2-5 child	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Strongly Agree
11	Married	Unemployed	1 only child	Agree	Agree	Agree	Agree	Agree	Neutral	Agree	Disagree	Agree
12	Married	Employed	2-5 child	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
13	Married	Employed	2-5 child	Strongly Agree	Strongly Agree	Neutral	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
14	Married	Employed	2-5 child	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Agree	Agree
15	Married	Employed	1 only child	Strongly Agree	Strongly Agree	Agree	Agree	Agree	Agree	Agree	Agree	Agree
16	Widowed	Employed	2-5 child	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Neutral	Agree	Agree	Agree
17	Married	Student	No child yet	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
18	Married	Unemployed	2-5 child	Neutral	Strongly Agree	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral
19	Married	Employed	2-5 child	Strongly Agree	Agree	Neutral	Agree	Agree	Neutral	Neutral	Neutral	Strongly Agree
20	Married	Unemployed	2-5 child	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral
21	Married	Employed	No child yet	Strongly Agree	Strongly Agree	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral
22	Married	Unemployed	No child yet	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
23	Married	Employed	No child yet	Strongly Agree	Strongly Agree	Neutral	Neutral	Strongly Agree	Neutral	Strongly Agree	Neutral	Neutral
24	Single Parent	Employed	2-5 child	Agree	Agree	Agree	Agree	Agree	Agree	Agree	Disagree	Agree
25	Married	Unemployed	2-5 child	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Neutral	Strongly Agree	Strongly Agree

Figure 5.3 : View detail of Parenting Observation Data

```

> CCE<- read_csv("cyberCrime_Experience.csv")
Rows: 142 Columns: 12
-- Column specification -----
Delimiter: ","
chr (12): Age, Occupation, C1, C2, C3, Experience, Type_Exp, E1, E...

i Use `spec()` to retrieve the full column specification for this data.
i specify the column types or set `show_col_types = FALSE` to quiet this message.
> summary(CCE)
  Age      Occupation      C1
Length:142 Length:142 Length:142
Class :character Class :character Class :character
Mode :character  Mode :character  Mode :character
  C2      C3      Experience
Length:142 Length:142 Length:142
Class :character Class :character Class :character
Mode :character  Mode :character  Mode :character
  Type_Exp      E1      E2
Length:142 Length:142 Length:142
Class :character Class :character Class :character
Mode :character  Mode :character  Mode :character
  E3      E4      E5
Length:142 Length:142 Length:142
Class :character Class :character Class :character
Mode :character  Mode :character  Mode :character
> View(CCE)
> |

```

Figure 5.4 : Summary Coding for Cybercrime Experience

	Age	Occupation	C1	C2	C3	Experience	Type_Exp	E1	E2	E3	E4	E5
1	18 - 25 years old	Student	No	Maybe	Yes	1 time	Theft Information, Hackers	Yes	No	No	No	No
2	18 - 25 years old	Student	Yes	Yes	Yes	2 - 5 times	Fraud, Phishing Attack	No	No	Yes	Yes	Yes
3	18 - 25 years old	Employed	Yes	Yes	No	Never	Fraud, Cyber Gambling, Pornography, Phishing Attack	No	Yes	Yes	Yes	No
4	18 - 25 years old	Employed	Yes	No	Yes	Never	Phishing Attack	No	No	No	No	No
5	18 - 25 years old	Student	No	Yes	Yes	1 time	Theft Information, Phishing Attack, Ransomware Attack	Yes	No	No	No	No
6	18 - 25 years old	Student	Yes	Maybe	Yes	2 - 5 times	Phishing Attack	No	No	No	No	No
7	9-17 years old	Student	Maybe	No	Maybe	Never	Fraud	Prefer not to answer	Prefer not to answer	No	Prefer not to answer	No
8	18 - 25 years old	Student	No	No	No	Never	Phishing Attack	No	No	No	No	No
9	36 and above	Employed	Yes	Yes	Yes	2 - 5 times	Phishing Attack	No	No	Yes	Yes	No
10	26 - 35 years old	Employed	Yes	Yes	Yes	More than 5 times	Phishing Attack	No	No	No	No	No
11	18 - 25 years old	Student	No	No	No	Never	Hackers, Phishing Attack	No	No	No	Yes	No
12	18 - 25 years old	Student	Maybe	Yes	Yes	2 - 5 times	Fraud, Phishing Attack	No	No	No	No	No
13	36 and above	Employed	No	No	No	2 - 5 times	Fraud, Cyber Gambling, Hackers, Phishing Attack	No	No	No	No	Yes
14	18 - 25 years old	Unemployed	No	Yes	Yes	2 - 5 times	Fraud, Cyber Gambling, Pornography, Hackers, Phishing A...	Yes	No	Yes	Yes	Yes
15	18 - 25 years old	Student	Maybe	Yes	Yes	1 time	Fraud	No	No	No	No	Yes
16	26 - 35 years old	Employed	Maybe	Yes	Yes	2 - 5 times	Fraud, Theft Information, Hackers, Phishing Attack	No	No	No	No	No
17	18 - 25 years old	Student	Yes	Yes	Yes	2 - 5 times	Cyber Gambling, Theft Information, Phishing Attack	Yes	No	Yes	Yes	No
18	18 - 25 years old	Student	No	No	Yes	1 time	Fraud	Yes	No	No	No	No
19	18 - 25 years old	Student	No	Yes	Yes	More than 5 times	Fraud, Theft Information, Phishing Attack	Yes	No	Yes	No	Yes
20	18 - 25 years old	Student	Maybe	Maybe	Maybe	Never	Fraud, Cyber Gambling, Pornography, Theft Information,...	No	No	Yes	Yes	No
21	18 - 25 years old	Student	Maybe	Yes	Yes	2 - 5 times	Fraud, Cyber Gambling, Pornography, Theft Information...	Yes	Yes	Yes	Yes	Yes
22	18 - 25 years old	Student	Maybe	No	Yes	Never	Cyber Gambling, Pornography	No	Yes	No	No	No
23	18 - 25 years old	Student	No	No	Maybe	2 - 5 times	Hackers, Phishing Attack	Yes	No	Yes	Yes	No
24	18 - 25 years old	Student	Maybe	Yes	Yes	2 - 5 times	Fraud, Phishing Attack	No	No	No	Yes	No
25	18 - 25 years old	Student	No	No	Yes	Never	Phishing Attack	No	No	No	No	No

Showing 1 to 26 of 142 entries, 12 total columns

```

Console Terminal Jobs
~/responder/
> View(CCE)
> |

```

Figure 5.5 : View data of Cybercrime Experience Data


```

> TS<- read_csv("Threat_Severity.csv")
Rows: 142 Columns: 11
-- Column specification -----
Delimiter: ","
chr (11): Age, Occupation, T1, T2, T3, T4, T5, T6, T7, T8, T9

i Use `spec()` to retrieve the full column specification for this data.
i specify the column types or set `show_col_types = FALSE` to quiet this message.
> summary(TS)
  Age                Occupation                T1
Length:142          Length:142              Length:142
Class :character    Class :character    Class :character
Mode :character      Mode :character     Mode :character
  T2                T3                T4
Length:142          Length:142          Length:142
Class :character    Class :character    Class :character
Mode :character      Mode :character     Mode :character
  T5                T6                T7
Length:142          Length:142          Length:142
Class :character    Class :character    Class :character
Mode :character      Mode :character     Mode :character
  T8                T9
Length:142          Length:142
Class :character    Class :character
Mode :character      Mode :character
> view(TS)
> |

```

Figure 5.6 : Summary Coding for Threat Severity Cybercrime

Age	Occupation	T1	T2	T3	T4	T5	T6	T7	T8	T9
1 18 - 25 years old	Student	Agree	Agree	Strongly Disagree	Agree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree
2 18 - 25 years old	Student	Strongly Agree	Strongly Agree	Strongly Disagree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree
3 18 - 25 years old	Employed	Strongly Agree	Disagree	Agree	Strongly Agree	Strongly Disagree	Agree	Neutral	Strongly Disagree	Strongly Agree
4 18 - 25 years old	Employed	Strongly Agree	Strongly Disagree	Neutral	Strongly Agree	Neutral	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree
5 18 - 25 years old	Student	Agree	Disagree	Strongly Disagree	Agree	Disagree	Strongly Agree	Agree	Disagree	Agree
6 18 - 25 years old	Student	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree	Strongly Disagree	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree
7 9 - 17 years old	Student	Neutral	Neutral	Agree	Neutral	Agree	Neutral	Neutral	Disagree	Neutral
8 18 - 25 years old	Student	Agree	Agree	Neutral	Agree	Agree	Agree	Agree	Disagree	Neutral
9 36 and above	Employed	Strongly Agree	Neutral	Agree	Neutral	Neutral	Strongly Agree	Strongly Agree	Neutral	Agree
10 26 - 35 years old	Employed	Agree	Disagree	Strongly Disagree	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral
11 18 - 25 years old	Student	Strongly Agree	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree
12 18 - 25 years old	Student	Strongly Agree	Strongly Disagree	Neutral	Strongly Disagree	Strongly Agree	Strongly Disagree	Strongly Agree	Strongly Agree	Disagree
13 36 and above	Employed	Agree	Agree	Neutral	Agree	Agree	Agree	Neutral	Agree	Agree
14 18 - 25 years old	Unemployed	Strongly Agree	Strongly Agree	Disagree	Strongly Agree	Agree	Agree	Disagree	Neutral	Neutral
15 18 - 25 years old	Student	Strongly Agree	Disagree	Strongly Disagree	Strongly Agree	Neutral	Strongly Agree	Disagree	Strongly Agree	Agree
16 26 - 35 years old	Employed	Agree	Strongly Disagree	Agree	Strongly Agree	Agree	Disagree	Strongly Disagree	Strongly Disagree	Neutral
17 18 - 25 years old	Student	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Neutral	Strongly Agree
18 18 - 25 years old	Student	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral
19 18 - 25 years old	Student	Strongly Agree	Agree	Strongly Disagree	Strongly Agree	Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree
20 18 - 25 years old	Student	Strongly Agree	Strongly Agree	Strongly Disagree	Strongly Agree	Strongly Disagree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Agree
21 18 - 25 years old	Student	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
22 18 - 25 years old	Student	Agree	Disagree	Neutral	Agree	Disagree	Strongly Agree	Strongly Disagree	Neutral	Neutral
23 18 - 25 years old	Student	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Agree	Strongly Agree
24 18 - 25 years old	Student	Agree	Neutral	Neutral	Strongly Agree	Disagree	Disagree	Neutral	Neutral	Agree
25 18 - 25 years old	Student	Agree	Agree	Agree	Agree	Agree	Agree	Agree	Agree	Agree

Showing 1 to 26 of 142 entries, 11 total columns

```

Console Terminal Jobs
~/responder/
> view(TS)
> |

```

Figure 5.7 : View Detail of Threat Severity Cybercrime Data

```

> SE<- read_csv("Self_Efficacy.csv")
Rows: 142 Columns: 21
-- Column specification -----
Delimiter: ","
chr (21): Age, Occupation, Exp_Situation, S1, S2, S3, S4, S5, S6, ...

i Use `spec()` to retrieve the full column specification for this data.
i Specify the column types or set `show_col_types = FALSE` to quiet this message.
> summary(SE)
  Age           Occupation      Exp_Situation
Length:142     Length:142      Length:142
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
  S1           S2           S3
Length:142     Length:142      Length:142
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
  S4           S5           S6
Length:142     Length:142      Length:142
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
  S7           S8           F1
Length:142     Length:142      Length:142
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
  F2           F3           F4
Length:142     Length:142      Length:142
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
  F5           F6           F7
Length:142     Length:142      Length:142
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
  F8           F9           Advice
Length:142     Length:142      Length:142
Class :character Class :character Class :character
Mode :character Mode :character Mode :character
> view(SE)
|

```

Figure 5.8 : Summary Coding for Self-Efficacy

	Age	Occupation	Exp_Situation	S1	S2	S3	S4	S5	S6	S7	S8	F1	F2
1	18 - 25 years old	Student	Trojan or malware, Auto generated mails to your inbox (...)	Good	Very Good	Good	Good	Very Good	Very Good	Good	Good	Disagree	Agree
2	18 - 25 years old	Student	Trojan or malware, Auto generated mails to your inbox (...)	Good	Very Good	Good	Good	Very Good	Good	Very Good	Good	Disagree	Strongly Disagree
3	18 - 25 years old	Employed	Trojan or malware, Auto generated mails to your inbox (...)	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Good	Neutral	Agree
4	18 - 25 years old	Employed	Never experienced such situation (Tidak pernah mengala...	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Disagree	Strongly Agree
5	18 - 25 years old	Student	Trojan or malware, Auto generated mails to your inbox (...)	Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Strongly Disagree	Agree
6	18 - 25 years old	Student	Auto generated mails to your inbox (Mel yang dijana sec...	Very Good	Very Good	Ok	Very Good	Very Good	Very Good	Very Good	Very Good	Strongly Agree	Strongly Agree
7	9 -17 years old	Student	Publishing obscure material on your profiles (Menerbitk...	Very Good	Ok	Ok	Ok	Ok	Ok	Ok	Ok	Neutral	Neutral
8	18 - 25 years old	Student	Never experienced such situation (Tidak pernah mengala...	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Agree	Agree
9	36 and above	Employed	Never experienced such situation (Tidak pernah mengala...	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Agree	Strongly Agree
10	26 - 35 years old	Employed	Never experienced such situation (Tidak pernah mengala...	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Strongly Agree	Strongly Agree
11	18 - 25 years old	Student	Never experienced such situation (Tidak pernah mengala...	Ok	Very Good	Very Good	Very Good	Very Good	Poor	Very Good	Ok	Strongly Disagree	Strongly Agree
12	18 - 25 years old	Student	Never experienced such situation (Tidak pernah mengala...	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Strongly Agree	Strongly Agree
13	36 and above	Employed	Auto generated mails to your inbox (Mel yang dijana sec...	Good	Good	Good	Good	Good	Good	Good	Good	Agree	Agree
14	18 - 25 years old	Unemployed	Trojan or malware, Confidential reports/ Information bei...	Good	Good	Good	Good	Good	Good	Good	Good	Neutral	Agree
15	18 - 25 years old	Student	Never experienced such situation (Tidak pernah mengala...	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Agree	Neutral
16	26 - 35 years old	Employed	Trojan or malware, Auto generated mails to your inbox (...)	Very Good	Very Good	Very Good	Very Good	Very Good	Ok	Very Good	Good	Neutral	Neutral
17	18 - 25 years old	Student	Trojan or malware, Auto generated mails to your inbox (...)	Very Good	Very Good	Ok	Good	Very Good	Ok	Very Good	Ok	Neutral	Neutral
18	18 - 25 years old	Student	Never experienced such situation (Tidak pernah mengala...	Ok	Ok	Ok	Ok	Ok	Ok	Ok	Ok	Neutral	Neutral
19	18 - 25 years old	Student	Trojan or malware, Auto generated mails to your inbox (...)	Very Good	Good	Very Good	Good	Good	Good	Very Good	Good	Strongly Disagree	Strongly Agree
20	18 - 25 years old	Student	Auto generated mails to your inbox (Mel yang dijana sec...	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Neutral	Strongly Agree
21	18 - 25 years old	Student	Auto generated mails to your inbox (Mel yang dijana sec...	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Strongly Agree	Strongly Agree
22	18 - 25 years old	Student	Never experienced such situation (Tidak pernah mengala...	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Very Good	Neutral	Agree
23	18 - 25 years old	Student	Confidential reports/ Information being hacked (Lapora...	Good	Good	Good	Good	Good	Good	Good	Good	Disagree	Strongly Agree
24	18 - 25 years old	Student	Publishing obscure material on your profiles (Menerbitk...	Very Good	Good	Very Good	Good	Good	Good	Very Good	Very Good	Agree	Neutral
25	18 - 25 years old	Student	Never experienced such situation (Tidak pernah mengala...	Very Good	Very Good	Good	Good	Good	Good	Good	Good	Agree	Agree

Figure 5.9 : View Detail of Self-Efficacy Data

5.5.3 Coding for RStudio

```
install.packages("readr")
library(readr)
data<- read_csv("responder/Data.csv")
summary(data)
View(data)

setwd("C:/Users/syafi/OneDrive/Documents/responder")

install.packages("tidyr")
install.packages("dplyr")
install.packages("tidyverse")
install.packages("ggplot2")
install.packages("readr")
install.packages("gridExtra")
library(tidyr)
library(dplyr)
library(tidyverse)
library(ggplot2)
library(readr)
library(gridExtra)
data<- read_csv("Data.csv")
summary(data)
View(data)

ggplot(data,aes(x=Age, y=Occupation))+geom_point()
ggplot(data,aes(x=Age, y=Occupation,col=Status))+geom_point()
ggplot(data,aes(x=Age, y=Occupation,col=Status))+geom_point(shape=15, size=4)

ggplot(data,aes(x=Age, y=Occupation,col=Status))+geom_point(shape=15, size=4) + ggtitle("Data
response Analysis \n Data Source : Google Form Survey")

ggplot(data,aes(x=S1, y=Status,col=Occupation))+geom_point(shape=15, size=4) + ggtitle("Data
response Analysis \n Data Source : Google Form Survey") + theme(plot.title = element_text(size=14,
lineheight = 0.8,hjust = 0.5))
```

```
ggplot(data,aes(x=Age, y=Type_Exp,col=Occupation))+geom_point(shape=15, size=0.5) + ggtitle("Data  
response Analysis \n Data Source : Google Form Survey") + theme(plot.title = element_text(size=14,  
lineheight = 0.8,hjust = 0.5))
```

```
PO<- read_csv("ParentObserve.csv")
```

```
summary(PO)
```

```
View(PO)
```

```
ggplot(PO,aes(x=P1, y=Status, col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Parenting  
Observation \n Limited the Amount of Time Their Spend on Gadget") + theme(plot.title =  
element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(PO,aes(x=P2, y=Status,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Parenting  
Observation \n Checked the Browser History to See Which Sites they Visited") + theme(plot.title =  
element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(PO,aes(x=P3, y=Status,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Parenting  
Observation \n Parenting Knowing Their Children's Online Passwords") + theme(plot.title =  
element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(PO,aes(x=P4, y=Status,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Parenting  
Observation \n Using Internet Filtering Software on Devices that Access") + theme(plot.title =  
element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(PO,aes(x=P5, y=Status,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Parenting  
Observation \n Having Online Rules Agreement with Children") + theme(plot.title =  
element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(PO,aes(x=P6, y=Status,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Parenting  
Observation \n Know Children Spend Chatting Online Time") + theme(plot.title = element_text(size=14,  
lineheight = 0.8,hjust = 0.5))
```

```
ggplot(PO,aes(x=P7, y=Status,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Parenting  
Observation \n The Devices Children kept In High Traffic Area") + theme(plot.title =  
element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(PO,aes(x=P8, y=Status,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Parenting  
Observation \n Allowing Children To Sownload Any Game Apps") + theme(plot.title =  
element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(PO,aes(x=P9, y=Status,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Parenting  
Observation \n Children Know of the Safety Tips") + theme(plot.title = element_text(size=14, lineheight  
= 0.8,hjust = 0.5))
```

```
CCE<- read_csv("CyberCrime_Experience.csv")
```

```
summary(CCE)
```

```
View(CCE)
```

```
ggplot(CCE,aes(x=C1, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Cyber Crime Experience \n Having Prior Knowledge About Criminology") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(CCE,aes(x=C2, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Cyber Crime Experience \n Having Any Experience in Cyber Crime") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(CCE,aes(x=C3, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Cyber Crime Experience \n Have Antivirus Software Installed on Device") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(CCE,aes(x=E1, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Cyber Crime Experience \n Beening Cyberbullied Victim") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(CCE,aes(x=E3, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Cyber Crime Experience \n Someone Pretended to be Online") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(CCE,aes(x=E4, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Cyber Crime Experience \n Someone sent A Sexual Content Message") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(CCE,aes(x=E5, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Cyber Crime Experience \n Victim of Fraud Online and Lost Money") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
TS<- read_csv("Threat_Severity.csv")
```

```
summary(TS)
```

```
View(TS)
```

```
ggplot(TS,aes(x=T1, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Threat Severity Cyber Crime \n Heard of Someone Being a Victim of Cyber Crime") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(TS,aes(x=T2, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Threat Severity Cyber Crime \n Been Hacked Through Email, Social Net / Blogs") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```
ggplot(TS,aes(x=T3, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Threat Severity Cyber Crime \n Allow Others to use Personal ID") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
```

```

ggplot(TS,aes(x=T4, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Threat Severity
Cyber Crime \n Seen Anything on the news about People Being Harassed Online") + theme(plot.title =
element_text(size=14, lineheight = 0.8,hjust = 0.5))

ggplot(TS,aes(x=T5, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Threat Severity
Cyber Crime \n Found Someone using or duplicate Personal detail ") + theme(plot.title =
element_text(size=14, lineheight = 0.8,hjust = 0.5))

ggplot(TS,aes(x=T6, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Threat Severity
Cyber Crime \n Found Someone Using Personal Detail and Report to Admin Website") + theme(plot.title =
element_text(size=14, lineheight = 0.8,hjust = 0.5))

ggplot(TS,aes(x=T7, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Threat Severity
Cyber Crime \n Feel Safe personal detail When Online") + theme(plot.title = element_text(size=14,
lineheight = 0.8,hjust = 0.5))

ggplot(TS,aes(x=T8, y=Occupation,col=Age))+geom_point(shape=15, size=3) + ggtitle("Threat Severity
Cyber Crime \n Lost Money due to Cyber Crime") + theme(plot.title = element_text(size=14, lineheight
= 0.8,hjust = 0.5))

SE<- read_csv("Self_Efficacy.csv")
summary(SE)
View(SE)

ggplot(SE,aes(x=S1, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Use strong password") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
ggplot(SE,aes(x=S2, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n activating firewall and use antivirus") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust =
0.5))
ggplot(SE,aes(x=S3, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n block Spyware attack") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
ggplot(SE,aes(x=S4, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Secure Mobile Devices") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))
ggplot(SE,aes(x=S5, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Uupdate Software and install the latest one") + theme(plot.title = element_text(size=14, lineheight =
0.8,hjust = 0.5))
ggplot(SE,aes(x=S6, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Protect data by Encryption sensitive files") + theme(plot.title = element_text(size=14, lineheight =
0.8,hjust = 0.5))
ggplot(SE,aes(x=S7, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Review bank statement Regularly") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust =
0.5))

```

```

ggplot(SE,aes(x=S8, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Secure Wireless Network") + theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))

ggplot(SE,aes(x=F1, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Created Trustworthy online Friendship with Strangers") + theme(plot.title = element_text(size=14,
lineheight = 0.8,hjust = 0.5))

ggplot(SE,aes(x=F2, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Ignored Emails from reputable Organizations with Odd/Excellent News") + theme(plot.title =
element_text(size=14, lineheight = 0.8,hjust = 0.5))

ggplot(SE,aes(x=F3, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Respond to SMS messages Advertising Competitions Offering Significant Prizes") + theme(plot.title
= element_text(size=14, lineheight = 0.8,hjust = 0.5))

ggplot(SE,aes(x=F4, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Never Rely on Strangers' Online Identity Disclosures") + theme(plot.title = element_text(size=14,
lineheight = 0.8,hjust = 0.5))

ggplot(SE,aes(x=F5, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Never think About Paying Any Money for Services Provided by An Internet Website") +
theme(plot.title = element_text(size=14, lineheight = 0.8,hjust = 0.5))

ggplot(SE,aes(x=F6, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Willing to Agree with Internet Pals' Requests to Deposit Money ") + theme(plot.title =
element_text(size=14, lineheight = 0.8,hjust = 0.5))


ggplot(SE,aes(x=F7, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Aware Capable of Spotting the Most Recent Internet Frauds") + theme(plot.title =
element_text(size=14, lineheight = 0.8,hjust = 0.5))

ggplot(SE,aes(x=F8, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Accept Strangers' Photos onthe Internet") + theme(plot.title = element_text(size=14, lineheight =
0.8,hjust = 0.5))

ggplot(SE,aes(x=F9, y=Age,col=Occupation))+geom_point(shape=15, size=3) + ggtitle("Self-Efficacy
\n Wouldn't Hesitate to Meet Up with Online Pals in Person") + theme(plot.title = element_text(size=14,
lineheight = 0.8,hjust = 0.5))

```

5.5.4 Proof of Survey



Cybercrime Behaviour During Pandemic Covid-19 in Malaysia

Dear respected respondents,
Assalamualaikum and Greetings Everyone!

My name is Nurul Syafiqah Binti Samsu, I am Bachelor of Computer Science (Computer System & Networking) from Universiti Malaysia Pahang (UMP) currently conducting a research study for my final year project under supervision Dr. Syafiq Binti Izhar Hisham (Faculty of Computing). Specifically, my research is to predict the criminology of cybercrime behaviour during pandemic covid-19 in Malaysia. This study is to fulfill the qualification as Bachelor of Computer Science student in Universiti Malaysia Pahang (UMP).

The goal of the research is to examine Malaysia's awareness of cybercrime behaviour during pandemic COVID-19. The main intent of this study is educational. As a result, I would greatly appreciate it if you took the time to complete ALL of the survey's sections and questions. However, thank you for your time and effort given in order to fill in this questionnaire. Your assistance in this attempt is much appreciated.

Responden yang dihormati,
Assalamualaikum dan Salam Sejahtera Semuanya!

Nama saya Nurul Syafiqah Binti Samsu, saya mengambil Jurusan Sarjana Muda Sains Komputer (Komputer Sistem & Rangkaian) di Universiti Malaysia Pahang (UMP) sedang menjalankan kajian selidik untuk projek tahun akhir saya di bawah penyelia Dr. Syafiq Binti Izhar Hisham (Fakulti Pengkomputeran). Secara khusus, kajian ini adalah untuk meramalkan kriminologi tingkah laku jenayah siber semasa pandemik covid-19 di Malaysia serta bagi memenuhi kelayakan sebagai pelajar Sarjana Muda Sains Komputer di Universiti Malaysia Pahang (UMP).

Matlamat penyelidikan adalah untuk menguji kesedaran rakyat Malaysia terhadap tingkah laku jenayah siber semasa wabak COVID-19. Matlamat utama kajian ini adalah berdasarkan pendidikan. Hasilnya, saya amat menghargai jika anda dapat meluangkan masa untuk melengkapkan SEMUA bahagian dan soalan tinjauan. Walau bagaimanapun, saya amat berterima kasih di atas masa dan usaha yang diberikan untuk mengisi borang soal selidik ini. Bantuan anda dalam percubaan ini amat dihargai.

If you have any questions, please contact me:
Nurul Syafiqah Binti Samsu
syafiqahsamsu@gmail.com

abangpiko123@gmail.com Switch account Draft saved
* Required

Email *
syafiqahsamsu@gmail.com

Next Clear form

Cybercrime Behaviour During Pandemic Covid-19 in Malaysia

abangpiko123@gmail.com Switch account
* Required

DEMOGRAPHIC PROFILE (PROFIL DEMOGRAFI)

Gender (Jantina) *

Male (Lelaki)
 Female (Perempuan)

Age (Umur) *

9 - 17 years old
 18 - 25 years old
 26 - 35 years old
 36 and above.

Race (Bangsa) *

Malay
 Chinese
 Indian
 Other

State (Negeri) *

Choose

Status *

Single (Bujang)
 Married (Berkahwin)
 Widowed (Janda / Duda)
 Single Mother/ Father (Ibu / Ayah Tunggal)

Occupation (Pekerjaan) *

Student (Pelajar)
 Employed (Bekerja)
 Unemployed (Tidak Bekerja)

Back Next Clear form

PARENTING OBSERVATION (PEMERHATIAN IBU BAPA)

This section will analyze parents' ability to monitor their children for protective and preventative actions against cybercrime. Please carefully study the statement on the efficacy of the answer to see how far you agree with it.

Bahagian ini akan menganalisis keupayaan ibu bapa untuk memantau anak-anak mereka untuk tindakan perlindungan dan pencegahan terhadap jenayah siber. Sila teliti kenyataan tentang keberkesanan jawapan untuk melihat sejauh mana anda bersetuju dengannya.

How many children do you have? *
Berapa bilangan anak anda?

No child yet
 1 only child
 2 - 5 child
 more than 5 child

Please tell us how much you agree or disagree with each statement.
Sila benthak kami sejauh mana anda bersetuju atau tidak bersetuju dengan setiap pernyataan.

	Strongly Agree	Agree	Neutral	Disagree	Very Disagree
Limited the amount of time their spend on gadget (Hadkan jumlah masa yang mereka luangkan untuk gajet)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Checked the browser history to see which sites they visited (Menyemak 'browser history' untuk melihat laman web yang mereka lawati)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Do you know your children's online passwords (Adakah anda tahu kata laluan dalam talian anak-anak anda)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Do you use internet filtering software on all devices your child has access to (Adakah anda menggunakan perisian penapisan internet pada semua peranti yang boleh diakses oleh anak anda)

Do you have an online rules agreement with your child (Adakah anda mempunyai perjanjian peraturan dalam talian dengan anak anda)

Do you know how many hours a week your child spends chatting online with others (Adakah anda tahu berapa jam dalam seminggu anak anda menghabiskan masa bersembang dalam talian dengan orang lain)

Is the devices your child uses kept in a high traffic area in your home (Adakah peranti yang digunakan anak anda disimpan di kawasan yang trafik tinggi di rumah anda)

Do you allow your child to download any game apps (Adakah anda membenarkan anak anda memuat turun sebarang app permainan)

Does your child know of the safety tips (Adakah anak anda tahu tentang petua keselamatan)

Back Next Clear form

CYBER CRIME EXPERIENCE (PENGALAMAN JENYAH SIBER)

This section is created to evaluate your level of understanding regarding cybercrime. Please read carefully to know your understanding based on your perspective.

Bahagian ini dicipta untuk menilai tahap pemahaman anda mengenai jenayah siber. Sila baca dengan teliti untuk mengetahui pemahaman anda berdasarkan perspektif anda.

Do you have prior knowledge about criminology?

Adakah anda mempunyai pengetahuan terdahulu tentang kriminologi?

- Yes (Ya)
 No (Tidak)
 Maybe (Mungkin)

Do you have any experience in cyber crime?

Adakah anda mempunyai pengalaman dalam jenayah siber?

- Yes (Ya)
 No (Tidak)
 Maybe (Mungkin)

How many times have you been a victim of cyber crime? *

Berapa kali anda menjadi mangsa jenayah siber?

- 1 time
 2 - 5 times
 More than 5 times
 Never

Which kind of cyber crime have you experienced? *

Jenayah siber yang manakah pernah anda alami?

(Can choose more than 1)

- Fraud (Penipuan)
 Cyber Gambling (Perjudian Siber)
 Pornography (Pornografi)
 Theft Information (Kecurian Maklumat)
 Hackers (Penggodam)
 Phising Attack (Spam)
 Ransomware Attack (Serangan Ransomware)
 Other: _____

Please read the statement about your experiences online carefully * to see how far you agree with it.

Sila baca kenyataan tentang pengalaman anda dalam talian dengan teliti untuk melihat sejauh mana anda bersetuju dengannya.

	Yes	No	Prefer not to answer
I've been cyberbullied victim (Saya pernah menjadi mangsa Siberbuli)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I've cyberbullied someone else. (Saya pernah Siberbuli seseorang)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Someone else has pretended to be online. (Seseorang telah menyamar menjadi saya dalam talian)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Someone has sent/share me messages with sexual content (Seseorang telah menghantar/berkongsi mesej dengan kandungan seksual kepada saya)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I've been the victim of fraud online and lost money. (Saya telah menjadi mangsa penipuan dalam talian dan kehilangan wang)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Back Next Clear form

THREAT SEVERITY CYBER CRIME

This section will go through the chance of a person becoming a victim of cybercrime.

Bahagian ini adalah peluang seseorang menjadi mangsa jenayah siber.

Please read the statement about threat vulnerability carefully to see * how far you agree with it.

Sila baca kenyataan tentang kelemahan ancaman dengan teliti untuk melihat sejauh mana anda bersetuju dengannya.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Have you ever heard of someone being a victim of cybercrime (Pernakah anda mendengar seseorang menjadi mangsa jenayah siber)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Have you ever been hacked through email, social net or blogs (Pernakah anda digodam melalui e-mel, jaringan sosial atau blog)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Do you allow others (Friends, relatives) to use your personal ID (Adakah anda membenarkan orang lain (Rakan, saudara mara) menggunakan ID peribadi anda)

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Have you seen anything on the news about people being harassed online (Pernakah anda melihat apa-apa mengenai berita tentang orang yang diganggu dalam talian)

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Have you found someone using your photo, profile, bank detail (in social network) or duplicating your personal details (Pernakah anda menemui seseorang menggunakan foto, profil, butiran bank anda (Dalam rangkaian sosial) atau menduplikasi butiran peribadi anda)

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

If you have found someone using your photo, profile, bank detail, did you report to admin website (Jika anda telah menemui seseorang menggunakan foto, profil, butiran bank anda, adakah anda melaporkan)

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Do you feel safe about your information when you online (Adakah anda berasa selamat tentang maklumat anda apabila anda dalam talian?)

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Have you ever lost money due to cyber crime (Adakah anda pernah kehilangan wang akibat jenayah siber)

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Do you feel it is essential to be safe online? (Adakah anda rasa keperluan asas untuk selamat dalam talian)

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Do you think that the laws in effect are able to control cyber criminal (Adakah anda berpendapat bahawa undang-undang)

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

SELF EFFICACY (KEBERKESANAN DIRI)

This section will explain about a person's ability to take precautions with their own device associated with the process and comfort when doing preventive actions online. Please read carefully how far you agree with the statement regarding self-efficacy based on your opinion.

Bahagian ini akan menerangkan tentang keupayaan seseorang untuk mengambil langkah berjaga-jaga dengan peranti mereka sendiri yang dikaitkan dengan proses dan keselesaan semasa melakukan tindakan pencegahan dalam talian. Sila baca dengan teliti sejauh mana anda bersetuju dengan kenyataan berkenaan keberkesanan diri berdasarkan pendapat anda.

Do you have an antivirus software installed on your PC/Mac? *

Adakah anda mempunyai perisian antivirus yang dipasang pada PC/Mac anda?

- Yes (Ya)
 No (Tidak)
 Maybe (Mungkin)

Have you ever experiences any of these situation? *

Adakah anda pernah mengalami mana-mana situasi ini?

- Trojan or malware
 Auto generated mails to your inbox (Mel yang dijana secara automatik ke peti masuk anda)
 Confidential reports/ Information being hacked (Laporan sulit/ Maklumat digodam)
 Publishing obscure material on your profiles (Menerbitkan bahan yang tidak jelas pada profil anda)
 Never experienced such situation (Tidak pernah mengalami situasi sedemikian)

Rate how much you protect your devices. *
Nilaiakan sejauh mana anda melindungi peranti anda.

	Very Good	Good	Ok	Poor	Very Poor
Use strong password by using combination of all (Gunakan kata laluan yang kuat dengan menggunakan gabungan semua)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

