

EMPLOYMENT FRAUD IN THE DIGITAL ERA:  
A STUDY OF UNIVERSITI KEBANGSAAN  
MALAYSIA STUDENTS' SUSCEPTIBILITY TO  
ONLINE JOB SCAMS

YAMUNAAH RANI A/P RAVICHANTHAR

UNIVERSITI KEBANGSAAN MALAYSIA

EMPLOYMENT FRAUD IN THE DIGITAL ERA:  
A STUDY OF UNIVERSITI KEBANGSAAN MALAYSIA STUDENTS'  
SUSCEPTIBILITY TO ONLINE JOB SCAMS

YAMUNAAH RANI A/P RAVICHANTHAR

PROJECT SUBMITTED IN PARTIAL FULFILMENT FOR THE DEGREE OF  
MASTER OF CYBER SECURITY

FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY  
UNIVERSITI KEBANGSAAN MALAYSIA

BANGI

2024

PENIPUAN PEKERJAAN DI ERA DIGITAL:  
KAJIAN TERHADAP KERENTANAN PELAJAR UNIVERSITI KEBANGSAAN  
MALAYSIA TERHADAP PENIPUAN KERJA ATAS TALIAN

YAMUNAAH RANI A/P RAVICHANTHAR

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN  
DARIPADA SYARAT MEMPEROLEH IJAZAH  
SARJANA KESELAMATAN SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT  
UNIVERSITI KEBANGSAAN MALAYSIA  
BANGI

2024

## DECLARATION

I hereby declare that the work in this project is my own except for quotations and summaries which have been duly acknowledged.

24 June 2024

YAMUNAAH RANI A/P RAVICHANTHAR

P111939

## ACKNOWLEDGEMENTS

First and foremost, I would like to thank my supervisor, Dr.Masnizah binti Mohd. for having me under her supervision. Without her support I would not have been able to complete this research. She was always there to help me and guide me in every way possible. She didn't limit me and always encouraged me to learn about new things that is related to this project.

I am grateful to my family, especially my husband, Saravanan for being there when things get hard and for always pushing me to be the better version of myself. For never giving up on me and always believing in me when I really needed it the most. Dad, G. Ravichanthar, I know you'll be there, always. Mum, L. Selvi, thank you for giving me your resilience.

To my brothers, Aravinthran, Karthi Raj, and Ravi Shangkar, thank you for believing in me always. I will always want to be a better person because of all of you. Thank you Yunesha for your support and love. Thank you to my in-laws for their understanding. Dimitri, for being the best part of my life.

Last but not least, thank you to everyone who helped me directly or indirectly upon completion of my research.

## ABSTRAK

Di dunia era digital kini, teknologi telah berkembang dengan ketara untuk memperbaiki kehidupan seharian kita dan segala urusan boleh dilakukan atas talian. Ia telah sampai ke tahap di mana kita tidak dapat lakukan urusan seharian tanpa teknologi walaupun kita mahu. Semua urusan telah didigitalkan, daripada lesen, perbankan, cukai jalan kenderaan, kursus dan kelas universiti, dan segalanya. Dengan peningkatan penggunaan internet, ancaman dalam talian juga meningkat. Kajian ini telah dilakukan untuk mengkaji kecenderungan pelajar Universiti Kebangsaan Malaysia (UKM) terhadap penipuan atas talian melalui tiga siri simulasi pancingan data spesifik iaitu Penipuan Pekerjaan, Tetapan Semula Kata Laluan, dan Tinjauan COVID-19. Objektif kajian ini termasuk, mereka bentuk dan analisis menggunakan pelbagai jenis kempen pancingan data (Penipuan Kerja, Tetapan Semula Kata Laluan dan Tinjauan COVID-19), menganalisis tahap kerentanan pelajar UKM, dan menilai keberkesanan kempen-kempen tersebut. Templat e-mel untuk kempen pancingan data ini dicipta dengan menggabungkan nada yang berbeza, nada positif untuk e-mel pancingan data Penipuan Kerja kerana ia menawarkan peluang pekerjaan sambilan yang lumayan, nada negatif untuk e-mel pancingan data Tetapan Semula Kata Laluan kerana ia menggesa pelajar bertindak segera dengan mewujudkan panik bahawa telah berlaku pelanggaran keselamatan dalam sistem UKM, dan akhirnya nada neutral untuk e-mel pancingan data Tinjauan COVID-19 kerana tidak ada implikasi jika tidak membalas emel tersebut. Kajian ini melibatkan 601 pelajar UKM, dibahagikan kepada tiga kumpulan berbeza. Ketiga-tiga kumpulan pelajar menerima ketiga-tiga e-mel pancingan data tanpa susunan tertentu. Data kajian telah dikumpul melalui simulasi dan tinjauan menggunakan pendekatan kuantitatif, mendedahkan pandangan berharga tentang tingkah laku pelajar UKM dan kesedaran tentang ancaman pancingan data. Hasil kajian menunjukkan bahawa simulasi pancingan data melalui Penipuan Pekerjaan memang mempunyai kadar penglibatan yang lebih tinggi dengan 16.8% pelajar mengklik pautan dan 12.1% pelajar menghantar data mereka berbanding dengan simulasi pancingan data Tetapan Semula Kata Laluan di mana 6% pelajar mengklik pautan dan 3.8% pelajar menghantar data mereka. Manakala bagi simulasi pancingan data Tinjauan COVID-19, 4.3% pelajar mengklik pautan pancingan data dan hanya 2.3% pelajar menghantar data mereka. Kajian ini menyumbang untuk meningkatkan kesedaran keselamatan siber dalam kalangan pelajar dan mencadangkan strategi untuk mengurangkan risiko berkaitan dengan penipuan pekerjaan dalam talian.

## ABSTRACT

We are living in the era of digital, where technology has advanced significantly to better our daily life. Everything can be done online. It came to a point where we are unable to live without technology even if we wanted to. Everything had been digitalized, from our license, to banking, to vehicle road tax, to university courses and classes, and the list goes on. With the rise of internet usage, online threats have risen as well. This study examines the susceptibility of Universiti Kebangsaan Malaysia (UKM) students to online scams through three types of spear phishing simulations which were Job Scam, Password Reset, and COVID-19 survey. The objectives include designing and evaluating using different types of phishing campaigns (Job Scams, Password Reset, and COVID-19 survey), analysing the susceptibility levels of UKM students, and assessing the effectiveness of these campaigns. The email templates for these phishing campaigns were created by incorporating different tones, positive tone for Job Scam phishing email as it offers lucrative part-time job opportunity, negative tone for Password Reset phishing email as it urges students to act immediately by creating a panic that there had been a security breach in the UKM system, and finally neutral tone for COVID-19 survey phishing email as there were no consequences for not responding. This study included 601 UKM students, separated into three different groups. All three groups of students received all three phishing emails with no particular order. Data was collected through simulations and survey using a quantitative approach, revealed valuable insights into UKM students' behaviours and awareness of phishing threats. The research findings demonstrated that Job Scam phishing simulations do indeed have higher engagement rate with 16.8% students clicked on the links and 12.1% students submitted their data compared to Password Reset where 6% of students clicked the links and 3.8% students submitted their data and for COVID-19 survey phishing simulations 4.3% students clicked on the phishing links and only 2.3% students submitted their data. The study contributes to enhance cybersecurity awareness among students and suggests strategies for mitigating the risks associated with online job scams.

## CONTENTS

		<b>Page</b>
<b>DECLARATION</b>		<b>iii</b>
<b>ACKNOWLEDGEMENTS</b>		<b>iv</b>
<b>ABSTRAK</b>		<b>v</b>
<b>ABSTRACT</b>		<b>vi</b>
<b>CONTENTS</b>		<b>vii</b>
<b>LIST OF TABLES</b>		<b>x</b>
<b>LIST OF ILLUSTRATIONS</b>		<b>xii</b>
<b>LIST OF ABBREVIATIONS</b>		<b>xvi</b>
<b>CHAPTER 1</b>	<b>INTRODUCTION</b>	
1.1	Research Background	1
1.2	Problem Statement	2
1.3	Research Questions	3
1.4	Research Objectives	4
1.5	Research Scope	4
1.6	Significance of Study	5
1.7	Thesis Outline	5
<b>CHAPTER II</b>	<b>LITERATURE REVIEW</b>	
2.1	Introduction	7
2.2	Types of Phishing Attacks	7
2.2.1	Email Spoofing	8
2.2.2	Social Engineering	8
2.2.3	Hacking	9
2.2.4	Investment Scam	10
2.2.5	Romance scam	11
2.2.6	Identity theft	12



2.3	University Students' Vulnerabilities and Responses to Online Scams	13
2.4	Deceptive Email Designs	16
2.5	Effectiveness of Different Spear Phishing Campaigns	24
2.6	Past Studies In UKM	25
2.7	Cybersecurity Awareness	26
2.8	Summary	28
<b>CHAPTER III</b>	<b>METHODOLOGY</b>	
3.1	Overview	29
3.2	Phase 1: Planning	31
	3.2.1 Target Group	32
3.3	Phase 2: Research Design	33
	3.3.1 Positive Phishing Campaign: Job Scam	35
	3.3.2 Negative Phishing Campaign: Urgent: Security Breach - Password Reset Required	36
	3.3.3 Neutral Phishing Campaign: Urgent: COVID-19 Vaccination Survey for Campus Safety	37
	3.3.4 Phishing Simulation Design	39
	3.3.4.1 GoPhish	39
	3.3.4.2 Amazon EC2	46
	3.3.5 Post Simulation Survey Design	47
3.4	Phase 3: Implementation	50
3.5	Phase 4: Data Analysis	51
3.6	Summary	52
<b>CHAPTER IV</b>	<b>RESULTS AND DISCUSSION</b>	
4.1	Introduction	53
	4.1.1 Job Scam Phishing Simulation Data Analysis	54
	4.1.2 Password Reset Phishing Simulation Data Analysis	56

	4.1.3	Covid-19 Survey Phishing Simulation Data Analysis	58
4.2		Demographic Data Analysis	61
	4.2.1	Gender	61
	4.2.2	Age	64
	4.2.3	Faculty	66
	4.2.4	Education Level	69
4.3		Post Simulation Survey Data Analysis	71
4.4		Discussion	87
4.5		Summary	90
<b>CHAPTER V</b>	<b>CONCLUSION</b>		
5.1		Introduction	91
5.2		Discussion	91
5.3		Contributions	93
5.4		Limitations and Future Work	94
<b>REFERENCES</b>			<b>95</b>
<b>APPENDICES</b>			
Appendix A1		Job Scam Phishing Campaign Google Form	101
Appendix A2		Password Reset Phishing Campaign Google Form	102
Appendix A3		COVID-19 Survey Phishing Campaign Google Form	103
Appendix B		Post Simulation Survey Google Form	105

**LIST OF TABLES**

<b>Table No.</b>		<b>Page</b>
Table 3.1	Sample Size	32
Table 3.2	Red Flag Indicator Table	34
Table 3.3	Job Scam Email Design	35
Table 3.4	Password Reset Email Design	37
Table 3.5	COVID-19 Survey Email Design	38
Table 3.6	Implementation Timeline	51
Table 4.1	Post Simulation Survey Question 1	72
Table 4.2	Post Simulation Survey Question 2	73
Table 4.3	Post Simulation Survey Question 3	74
Table 4.4	Post Simulation Survey Question 4	75
Table 4.5	Post Simulation Survey Question 5	76
Table 4.6	Post Simulation Survey Question 6	77
Table 4.7	Post Simulation Survey Question 7	78
Table 4.8	Post Simulation Survey Question 8	79
Table 4.9	Post Simulation Survey Question 9	80
Table 4.10	Post Simulation Survey Question 10	81
Table 4.11	Post Simulation Survey Question 11	82
Table 4.12	Post Simulation Survey Question 12	83
Table 4.13	Post Simulation Survey Question 13	84
Table 4.14	Post Simulation Survey Question 14	85

Table 4.15	Post Simulation Survey Question 15
------------	------------------------------------

86

## LIST OF ILLUSTRATIONS

<b>Figure No.</b>		<b>Page</b>
Figure 2.1	Phishing attack taxonomy adapted from (Almomani et al 2013, Rastenis et al. 2020)	19
Figure 3.1	Research Methodological Framework (Adapted from Creswell 2014, Siti Zaleha Binti Ahmad 2020)	31
Figure 3.2	Job Scam Phishing Email	36
Figure 3.3	Password Reset Phishing Email	37
Figure 3.4	COVID-19 Survey Phishing Email	38
Figure 3.5	GoPhish User Group Creation	39
Figure 3.6	GoPhish Sending profile	40
Figure 3.7	GoPhish Landing Page	41
Figure 3.8	Fake UKM Landing Page	42
Figure 3.9	Google Form Redirection	42
Figure 3.10	GoPhish Job Scam Email Template	43
Figure 3.11	GoPhish Password Reset Email Template	44
Figure 3.12	GoPhish COVID-19 Survey Email Template	45
Figure 3.13	AWS EC2 Dashboard	46
Figure 3.14	AWS EC2 Instance Details	46
Figure 3.15	GoPhish Server Host (Ubuntu)	47
Figure 3.16	Job Scam Google Form	48
Figure 3.17	Password Reset Google Form	48
Figure 3.18	COVID-19 Survey Google Form	48
Figure 3.19	Post Simulation Email	49

Figure 3.20	Post Simulation Google Form	50
Figure 4.1	Group 1 Job Scam Phishing Simulation Result from GoPhish	54
Figure 4.2	Group 2 Job Scam Phishing Simulation Result from GoPhish	54
Figure 4.3	Group 3 Job Scam Phishing Simulation Result from GoPhish	54
Figure 4.4	Job Scam Phishing Simulation Result	55
Figure 4.5	Group 1 Password Reset Phishing Simulation Result from GoPhish	56
Figure 4.6	Group 1 Password Reset Phishing Simulation Result from GoPhish 2.0	56
Figure 4.7	Group 2 Password Reset Phishing Simulation Result from GoPhish	56
Figure 4.8	Group 2 Password Reset Phishing Simulation Result from GoPhish 2.0	57
Figure 4.9	Group 3 Password Reset Phishing Simulation Result from GoPhish 2.0	57
Figure 4.10	Password Reset Phishing Simulation Result	57
Figure 4.11	Group 1 COVID-19 Survey Phishing Simulation Result from GoPhish	58
Figure 4.12	Group 1 COVID-19 Survey Phishing Simulation Result from GoPhish 2.0	59
Figure 4.13	Group 2 COVID-19 Survey Phishing Simulation Result from GoPhish	59
Figure 4.14	Group 3 COVID-19 Survey Phishing Simulation Result from GoPhish	59
Figure 4.15	COVID-19 Survey Phishing Simulation Result from GoPhish	60
Figure 4.16	Job Scam Phishing Simulation Result by Gender	61
Figure 4.17	Password Reset Phishing Simulation Result by Gender	62
Figure 4.18	COVID-19 Survey Phishing Simulation Result by Gender	63
Figure 4.19	Job Scam Phishing Simulation Result by Age	64

Figure 4.20	Password Reset Phishing Simulation Result by Age	65
Figure 4.21	COVID-19 Survey Phishing Simulation Result by Age	65
Figure 4.22	Job Scam Phishing Simulation Result by Faculty	66
Figure 4.23	Password Reset Phishing Simulation Result by Faculty	67
Figure 4.24	COVID-19 Survey Phishing Simulation Result by Faculty	68
Figure 4.25	Job Scam Phishing Simulation Result by Education Level	69
Figure 4.26	Password Reset Phishing Simulation Result by Education Level	70
Figure 4.27	COVID-19 Survey Phishing Simulation Result by Education Level	70
Figure 4.28	Post Simulation Survey Question 1	72
Figure 4.29	Post Simulation Survey Question 2	73
Figure 4.30	Post Simulation Survey Question 3	74
Figure 4.31	Post Simulation Survey Question 4	75
Figure 4.32	Post Simulation Survey Question 5	76
Figure 4.33	Post Simulation Survey Question 6	77
Figure 4.34	Post Simulation Survey Question 7	78
Figure 4.35	Post Simulation Survey Question 8	79
Figure 4.36	Post Simulation Survey Question 9	80
Figure 4.37	Post Simulation Survey Question 10	81
Figure 4.38	Post Simulation Survey Question 11	82
Figure 4.39	Post Simulation Survey Question 12	83
Figure 4.40	Post Simulation Survey Question 13	84
Figure 4.41	Post Simulation Survey Question 14	85
Figure 4.42	Post Simulation Survey Question 15	86

Figure 4.43 Overall Number of Clicked Links and Data Submitted

88



**LIST OF ABBREVIATIONS**

AOL	America Online
AWS	Amazon Web Services
Amazon EC2	Amazon Elastic Compute Cloud
CCID	Commercial Crime Investigation Department
COVID-19	Corona Virus Disease 2019
MyCERT	Malaysia Computer Emergency Response Team
PTM	Information Technology Center
UKM	Universiti Kebangsaan Malaysia
URL	Uniform Resource Locator

# CHAPTER I

## INTRODUCTION

### 1.1 Research Background

Cheating and scamming have always been part of human history long before the digital era. Evolving with time, people used various methods to cheat. However, they all have one common element: money. From ancient times till now, scammers have always found ways to swindle people out of their hard-earned money. Now, as technology advancement has skyrocketed, the methods of cheating and scamming have evolved significantly. Cybercriminals exploit digital platforms for financial profit with more sophisticated scams such as phishing attacks, malware, and ransomware.

Phishing attacks are one of the most popular and commonly used techniques by threat actors. It is often crafted to manipulate victims into revealing private information by creating messages that limit cognitive processing and promote quick, emotional responses (Harrison et al 2016, Workman 2008). Phishing attacks are a form of social engineering in which attackers impersonate trusted entities to manipulate victims into disclosing sensitive information, such as login credentials or financial data (Bitaab et al., 2020). The phrase "social engineering" refers to a deception tactic that takes advantage of human mistakes to get personal information, access, or assets (Almutairi & Alghamdi, 2022). It is a sort of cybercrime in which unwary people are persuaded to expose data, propagate malware infections, or grant access to restricted systems.

To steal personal information or money, cyber criminals target victims using phishing emails phone calls, or text messages. Individuals, organizations, and even governments can be the targets of social engineering assaults. Similarly, an organization or its workers are frequently targeted to get or gain access to sensitive information or systems. Over the last decade, spear phishing has emerged as a more targeted and sophisticated variant of phishing (Shashidhar 2017).

## **1.2 Problem Statement**

As the digital landscape continues to evolve, the prevalence of online scams has become a growing concern, particularly among university students. The COVID-19 pandemic has led to a surge in the use of the internet as many users relied on the internet for their work and studies. This has created an opportunity for threat actors to exploit individuals, including university students (Dé et al., 2020). Cyber attackers also frequently use phishing attacks to target university students. Although youngsters nowadays are tech-savvy, they are not exempt from these threats. Due to university students limited financial means, lack of experience, and increased daily reliance on digital technology, they became more vulnerable to online scams.

Some of the most common scams targeting university students are job scams such as pyramid schemes, too-good-to-be-true-offers, or fake job offers requiring upfront payment, fake scholarships and grants scams that requires upfront fees, and tech support scams that often involves in a pop-up message claiming that there's something wrong with the computer. University Kebangsaan Malaysia (UKM) students, who frequently engage in online activities for academic and personal purposes, are potential targets for such scams.

Email is the most widely used phishing method (Gomes, Reis, and Alturas 2020). Unlike traditional phishing emails that are sent in large volume targeting people randomly, spear phishing attacks are customized and tailored to specific individuals or

organizations. Typically, in spear phishing, the attacker does background research on the target before launching the attack to sound more convincing. After research, the attacker then sends emails to impersonate authority figure or trusted person. The attacker's main objective is to trick victims into clicking on malicious links or downloading malicious email attachments to reveal sensitive information such as login credentials or financial details.

Based on Malaysia Computer Emergency Response Team (MyCERT) reported incidents', in 2023, 3705 online fraud incidents were reported while 4741 online fraud incidents were reported in 2022. Although the number of fraud incidents have decreased, the difference between online fraud compared to other security incidents are relatively high. Online fraud incidents in 2023 makes up for 62.62% of the overall reported incidents. Moreover, online fraud had been consecutively high since 2016 among nine categories of reported incidents (MyCERT 2024).

### **1.3 Research Questions**

This research aims to answer three main questions relating to spear-phishing susceptibility. The research questions were formed after a thorough study of pass research pertaining to online scams involving students.

1. What are the elements that are most effective in designing realistic Job Scam, Password Reset, and COVID-19 survey phishing emails?
2. How susceptible are university students to job scam phishing campaigns compared to other types of phishing campaigns?
3. Which type of spear phishing campaign (Job Scam, Password Reset, and COVID-19 survey) has the highest success rate in deceiving UKM students?

#### **1.4 Research Objectives**

The objectives of this research are:

1. To design different types of spear phishing campaigns (Job Scam, Password Reset, and COVID-19 survey) for UKM students.
2. To analyse the susceptibility of UKM students to online scams via spear phishing.
3. To evaluate the effectiveness of different spear phishing campaigns (Job Scam, Password Reset, and COVID-19 survey) on UKM students.

#### **1.5 Research Scope**

The scope of this research is as following:

1. This research adapts the existing simulation procedure that was developed by Norhafizah Abu Bakar (2017).
2. This research aimed to conduct a phishing campaign involving UKM students.
3. Three types of phishing emails were used, Job Scams for positive tone, Password Reset for negative tone, and COVID-19 survey for neutral tone.
4. Data was collected through spear phishing simulations and post simulation survey, adopting a quantitative method.

## **1.6 Significance of Study**

This research contributes by assessing the susceptibility of UKM students to online job scams through spear phishing simulations. The study adapts from the previously conducted phishing simulations in UKM with different approaches. The result of this phishing campaign determines whether the phishing simulations should be conducted regularly involving all of UKM students. This study also highlights the importance of cybersecurity awareness among students. Students are indeed vulnerable to phishing attacks. Thus, a simulated phishing attack would help them to be more vigilant and recognize malicious emails or phishing attacks in the future.

Besides that, this research could set the base for UKM's Information Technology Center (PTM) to conduct regular phishing simulations for UKM students. The findings from the phishing simulations can help PTM to design awareness programs as well as focus more on the more vulnerable groups of students. Regular phishing campaigns will enable PTM to monitor the progress and the effectiveness of these programs and alter them as needed.

## **1.7 Thesis Outline**

This research consists of five chapters, the details of the chapters are as follow:

1. Chapter I is an introduction to the research topic, explaining the problem statement, research questions, research objectives, scope, and significance of this study.
2. Chapter II is literature review that discusses the research papers and journals pertaining to this study. It also includes an introduction to types of phishing attacks and literature studies related to the research questions.

3. Chapter III is about research methodology, where it describes the research flows and processes. This chapter also includes the designing of the phishing emails and survey questions.
4. Chapter IV is about the results and discussion for this project. It describes the results of this research based on the data that was collected throughout this research. The data was then analysed and discussed in this chapter.
5. Chapter V is the conclusion for this research and discusses the findings of this study. Besides that, it also contains limitations and recommendations for future research.

## **CHAPTER II**

### **LITERATURE REVIEW**

#### **2.1 Introduction**

This section covers the important findings from recent and previous studies on social engineering, cyber scam awareness, and cybersecurity. It will go over the many forms of phishing attacks, such as phishing scams, hacking, investment scams, romance scams, and identity theft. This section also shows university students' susceptibility and countermeasures to internet fraud, deceptive email designs, and effectiveness of different spear campaigns. At the same time, cybersecurity awareness will be explored by discussing fundamental cybersecurity knowledge, factors, and hurdles to cybersecurity awareness among students at universities.

#### **2.2 Types of Phishing Attacks**

In the age of the internet, cybercrime is a rising and dynamic menace, involving a wide variety of crimes carried out via electronic means. Understanding the various forms of cybercrime is critical for building effective preventive and response strategies. Fraudulent emails, bogus websites, and social engineering techniques are all common phishing techniques. Phishing is a fraudulent activity in which hackers pose as a trustworthy institution to steal sensitive information such as usernames, passwords, and financial information.



According to (Chaudhry, Chaudhry, and Rittenhouse 2016), normally a phishing attack consists of three things, a lure, a hook, and catch. The lure being the email sent to the victims to appear to be legitimate. The sender combines social engineering techniques with technology in order to lure and deceive their victims into disclosing private information. These emails typically involve emotions such as curiosity – links that lead to malicious websites, fear – urging users to share sensitive information, and empathy – impersonating a family member or friend for financial assistance. There are also other emotions used like lust, vanity, or greed. The email's compromised link or attachment serves as the hook, and the data collected and used by the attacker becomes the catch.

The following literature studies gives an overview of several common types of cybercrime.

### **2.2.1 Email Spoofing**

The incidence of cyber risks has increased considerably in the digital age when interactions and transactions occur at the speed of light. Email spoofing and phishing schemes are two of the most subtle and misleading strategies used by hackers. These unscrupulous methods take advantage of faith in electronic communication, posing major hazards to individuals, corporations, and even entire economies. According to Ramdinmawii et al., (2015), email spoofing is the practice of sending an email from one source that looks to have been received from another. Email spoofing is a common source of financial loss.

### **2.2.2 Social Engineering**

According to Jahankhani et al., (2014), phishing has become the most commonly used social engineering attack to date because it is quite simple to carry out and requires no direct communication between hacker and victim (i.e., a hacker does not need to phone

their prey, pretending to be a technical support staff, etc.). Sending bulk emails to thousands of prospective victims increases the likelihood of someone becoming a victim.

Conteh and Schmick (2016) stated that social engineering is the purposeful creation and implementation of deceptive strategies to manipulate human targets. In the domain of cyber security, it is generally used to persuade victims to provide private data or to perform acts that violate security regulations, such as accidentally infecting computers or leaking classified information.

Breda et al., (2017) added that social engineering attack is based on deception to evade cyber security mechanisms by exploiting the weakest link, which is the people involved. Victims are oblivious to the damaging nature of their acts during the engagement and the threat actor makes use of innocent tendencies. Explicit means such as threats or bribes are not covered under social engineering. A skilled practitioner of this profession recognizes and understands social interaction patterns to affect the psychological components of the human mind. With this resolution, the attacker may carry out an efficient and low-cost security compromise without having to invest in breaking technological security safeguards.

### **2.2.3 Hacking**

In the context of online scams, hacking is defined as the unauthorized access, manipulation, or exploitation of computer systems, networks, and online platforms to perpetrate fraud (Yar, 2006). Hackers frequently use numerous ways to acquire access to personal information, financial assets, or control over digital resources for unlawful reasons in online fraud. The assaults are carried out in stages, including information collection or reconnaissance, scanning, and eventually entry into the target system. Methods of getting information or opening security gaps are included in information gathering. It's quite similar to the way typical robberies are carried out. Before

attempting to rob a location, the thief will gather all relevant information (Jahankhani et al., 2014). In the same way, the computer attacker will strive to learn more about the target. An attacker could utilize social engineering to obtain information.

#### **2.2.4 Investment Scam**

The attractiveness of investing opportunities has spread beyond traditional channels in an interlinked and digital age. Unfortunately, this growth has resulted in a troubling phenomenon: sophisticated phishing attempts that permit investment schemes. Individuals' eagerness to increase their fortune or capitalize on financial possibilities is exploited by hackers, who use misleading techniques to entice naive victims into fake financial programs. Investment scams have long been a hazard, characterized by deceptive methods that promise substantial returns on investments. The use of phishing attacks by cyber deception to coordinate and perpetrate these frauds makes the present scenario extremely dangerous. Phishing adds another level of complexity, allowing fraudsters to personally target potential investors while often avoiding typical security safeguards. In the context of investment schemes, phishing attacks involve the use of false emails, messages, or websites impersonating respectable financial institutions, investment businesses, or trustworthy entities. These carefully prepared messages are designed to fool recipients into submitting critical financial information, login passwords, or even transferring cash to bogus accounts.

Lewis (2023) stated in an article that emphasizes the ubiquity of investment frauds on social media sites, which results in substantial financial losses for customers. According to the Federal Trade Commission, financial frauds, including cryptocurrency schemes, cost consumers \$3.8 billion in the United States alone last year, more than double from the previous year. Similarly, Zolkepli (2023) reported on an alarming surge in investment scam cases, with an average of 15 new cases investigated daily in 2023. Between January and October, a total of 4,435 cases were reported, resulting in over RM360 million in losses for victims. This represents a 54.1% increase in cases and a 93.6% spike in losses compared to the same period in the previous year. Investment

scams, primarily conducted online via social media platforms, accounted for 20% of total losses from commercial crime cases this year. According to Ramdinmawii et al., (2015), investment scams that are targeted at Americans include high-return or 'risk-free' investments, pyramid schemes, and 'Ponzi' schemes according to the U.S. Securities and Exchange Commission.

University students are common victims of investment scams since they are constantly seeking ways to earn money. When they come across websites that provide daily payment for simple tasks, they feel it is legitimate and try to get some pocket money from it. A college student lost approximately RM19000 in a part-time work fraud revealed on social media, according to a report by Devi (2023). Wendy, who was a student, replied to a Facebook post for a job in which she could earn commissions by providing nice evaluations for an airline firm. Wendy earned money and commissions after performing duties, according to a person purporting to be a firm employee. The sum she had to pay, however, increased with each work, forcing her to borrow money from a friend. Wendy eventually lost over RM15,000, including RM12,000 borrowed from a friend.

### **2.2.5 Romance scam**

Romance scams occur when fraudsters imitate another person by creating fake accounts and defrauding victims via dating or social networking platforms. Scammers frequently prey on their victims' emotional vulnerabilities, deceiving them for monetary benefits. According to Buchanan & Whitty, (2014), typically, the scammers profess they are in love with their prey at an early stage. They take the relationship' off the dating site and interact via Instant Messenger and email. Communication between fraudster and victim is regular and intensive throughout weeks, months, and sometimes years. Scammers may ask for little presents (e.g., a mobile phone or a new webcam) as a testing-the-water tactic as the 'relationship' develops. If the victim agrees to these requests, higher sums of money will be demanded. Third parties are frequently introduced into the story to make the fraud look more credible and to request money in novel ways.

Victims of romance scams may suffer significant emotional and financial effects. Individuals should always check the authenticity of internet connections and avoid providing money to anyone they haven't seen in person to avoid falling victim to such fraud. Combating the prevalence of romance fraud requires education and awareness.

### **2.2.6 Identity theft**

Identity theft, according to Jahankhani et al., (2014), is the act of collecting sensitive information about another person without their knowledge and utilising that information to perpetrate crime or fraud. The Internet has enabled cybercriminals to get such information from weak firms' databases. It has also allowed them to mislead victims into believing they are revealing sensitive private data to a trustworthy business or occasionally as a response to an e-mail requesting for revised billing or membership information, as well as an application to a (false) Internet job posting. A few types of identity theft were defined by Agbaje et al., (2015) which includes credit card fraud, phone and utilities fraud, bank fraud, employment fraud, government fraud and loan fraud.

As stated by Vadza (2011), identity theft is a vehicle for committing various forms of fraud schemes. Breda et al. (2017) examined identity theft in terms of impersonation in order to obtain credibility as a foundation for further hostile acts such as piggybacking, pretexting, and quid pro quo. Piggybacking, like tailgating, allows the attacker to obtain physical access to restricted places. However, in this scenario, obtains authorization from the individual with genuine access by impersonating corporate organisations such as staff that require temporary entrance. The primary objective of this attack is the creation of a believable scenario in order to engage the intended victim. In the context of social engineering and cyber security, this assault is usually disguised as a fake technological service that requires sensitive information to be successful.

### 2.3 University Students' Vulnerabilities and Responses to Online Scams

Susceptibility to deceit, according to Goel et al. (2017), is a primary source of security breaches owing to inherent human frailty. Hackers take advantage of this flaw by sending phishing emails that entice users to click on harmful links, which either download malware or deceive the victim into disclosing personal private information to the hacker. University students, like many other people, are vulnerable to different internet frauds owing to a number of circumstances. Camoens (2023) stated in a news article that according to the Bukit Aman Commercial Crime Investigation Department (CCID), about RM305.94 million was lost to e-commerce scams in Malaysia between 2021 and August 2023. E-commerce scams involve fraudulent online buying deals in which vendors offer phony things and disappear after receiving money, commonly on online or social media platforms. E-commerce frauds were recorded in 9,499 incidents in 2021, 9,253 in 2022, and 7,911 between January and August 2023.

Shadiqe (2023) revealed in an article that a 22-year-old university student fell prey to a job opportunity scam and nearly lost RM73,000. The fraud included a part-time job providing a substantial monthly salary over Telegram Messenger. The victim was promised a 10% profit on things listed online, but she had to buy the items herself. After believing the fraudster, the victim deposited RM72,877, only to discover that she had been duped when the promised things were not delivered and she earned no profit. Similarly, Wong (2023) reported on a university student in Sibul who lost RM13,180 as a result of an online part-time employment fraud. The victim was duped into joining a WhatsApp Group that advertised online part-time jobs, and the suspect commanded money transfers with promises of returns and commissions. The victim realised they were duped after completing chores and sending a total of RM13,180 into three bank accounts, as the promised commission was never paid.

This has raised interests in researchers to study the factors contributing to vulnerabilities against phishing or online scams amongst university students. Goel et al., (2017) studied the susceptibility of phishing on a targeted group of students based

on the contextualization of phishing emails. The authors evaluated the effects of changing the framing and content of email messages on consumers' susceptibility to phishing. They designed phishing emails to instil fear of losing something valued (e.g., course registrations, tuition help) or excitement of acquiring something desired (e.g., iPad, gift card, social networks). They built the tone of the emails to exploit human psychological flaws such as greed, social demands, and so forth. They sent bogus (harmless) emails to 7,225 undergraduate students and tracked their replies. The findings demonstrated that contextualizing communications to appeal to recipients' psychological flaws made them more vulnerable to phishing. The dread of losing or the anticipation of acquiring something important made people more vulnerable to deceit and phishing.

Similarly, a study conducted by Hassandoust et al., (2019) where they investigated how changing the framing and content of phishing communications influences individual vulnerability to phishing by using two fake phishing campaigns and an online survey. This study also took into account if there was a difference between how people are expected to react to phishing attacks and how they actually reacted. They discovered that individuals are more susceptible to phishing attacks when the phishing messages they get are tailored to their context, therefore appealing to their psychological weaknesses. There was also a big difference between how people were expected to react to phishing attacks and how they actually reacted. Finally, the researchers discover that these outcomes differ by gender.

A study conducted by Yoro et al., (2023) that evaluated the factors that contributed features to phishing vulnerability amongst students of a petroleum-related university in Nigeria determined that a combination of personal relevance, emotional gaps, and the fear factor extensively causes the efficacy rate of the phishing scheme. They discovered that higher computer usage and cyber-awareness were associated with reduced click rates. Students who were uninformed of phishing attacks outperformed those who were primed and knowledgeable of phishing attacks or who knew what phishing attacks they associated with.

By the same token, Bailey and Mitchell (2008) examined freshman and junior-level business core information system undergraduate students' vulnerability to phishing. It was determined that the study's respondents have a strong grasp of the dangers of replying to emails from what looks to be a financial organization. However, their smart decision-making abilities end there, as 88% of respondents fell victim to the URL masking tactic. This discovery was controversial owing to the widespread usage of URL masking. As a result, students are at risk of opening an attachment without first verifying that it was received by a friend.

On the other hand, Broadhurst et al. (2018) investigated phishing and cybercrime threats in a university student population of 138 people. To study their responses to social engineering and to investigate their attitudes towards cybercrime threats, the researchers sent three types of scam emails which were generic, customised, and targeted. According to the findings, international and first-year students were substantially more likely to be duped by scammers than local and second-year students. The most effective phishing scam was an urgent email sent during a test period concerning the participants' final exam agenda. The email became successful most likely because it was both relevant and salient, and it generated dread in participants since the email demanded immediate adjustments from them.

Based on the past studies and real-life examples, several important insights emerge regarding university students' susceptibility to online scams and phishing attacks. Human frailty is a significant factor. Human weaknesses such as fear and excitement are being exploited by hackers to influence individuals to click on malicious links or disclose personal information. Real-life cases reported by Shadiqe (2023) and Wong (2023) demonstrate that university students are particularly vulnerable to job scams, often losing substantial amounts of money to fraudulent job offers. E-commerce scams are also prevalent in Malaysia, with significant financial losses indicating a widespread threat.



A notable gap exists between how individuals expect to react to phishing attempts and their actual responses, highlighting the need for practical training and awareness programs. Despite students' understanding of email risks, many still fall victim to common tactics like URL masking, emphasizing the need for specific education on these methods. Overall, the findings shed light to the need for cybersecurity education, training programs, awareness campaigns, and promoting good cyber hygiene practices to reduce students' vulnerability to online scams and phishing attacks.

## **2.4 Deceptive Email Designs**

In today's tech-driven world, where a major part of our daily lives has transitioned online, the threat of phishing attacks has increased notably. Cybercriminals keep finding new ways and tactics to exploit people's fears, curiosity, and naiveness into revealing sensitive information. Phishing emails include a variety of manipulation strategies, like monetary rewards or creating a sense of urgency, to persuade recipients to reply (Burita et al. 2021). As such, phishing emails are becoming more sophisticated and harder to detect day by day.

Some of the recent studies have shed light on the growing challenges in detecting modern phishing attacks. Participants in these studies often struggled to identify phishing emails, especially the emails that seem to appear more authentic and trustworthy (Carroll, Adejobi, and Montasari 2022, Ferreira and Lenzini 2015). Undeniably, how successful spear phishing is determined by its ability to deceive its recipient.

A case study conducted by Yeoh et al. (2021) investigated the effectiveness of phishing awareness campaign at improving cybersecurity. The study was conducted over seven months and involved over 10,000 people across various campuses and offices worldwide representing a diverse range of professional and academic

departments. This was to ensure that that the study wasn't biased when it came to the demographic. The main objectives of the study were to reduce the number of people who respond to phishing emails, increase the number of people who report phishing emails, and to identify the most vulnerable group in the organization.

Prior to the phishing awareness campaign, 14 different types of phishing emails were sent out to establish a baseline. This was followed by a six-month campaign where each month, a new type of phishing email was sent out. Anyone who fell victim to the phishing email was immediately directed to a phishing education video created by the university's cybersecurity team. This immediate education training aimed to reinforce learning and promote behavioural change. The study measured participants' interactions with the phishing emails such as email replies, email opening, clicking on embedded links, opening of suspicious attachments, and phishing email reporting to the cybersecurity team. The phishing trainings aimed to reduce unsafe behaviour and increase phishing reporting rates.

The phishing emails were designed to deceive the participants into clicking on the suspicious links or opening the phishing attachments. There were four main components that was used in designing the phishing emails:

1. Mismatch name and email address
2. Misspellings, grammatical errors, incorrect spaces in the emails
3. The emails urge for immediate actions
4. The link text does not match the URL link that's displayed when hovering the cursor over it.

One of the critical elements in designing effective phishing emails is URL (Uniform Resource Locator) shortening. URL is a web address that enables online website location (Burita et al. 2021). URL shortening is mainly used to make an email seem more user-friendly and professional. However, shortened URL makes it difficult for users to identify the actual destination of a link. Threat actors take advantage of this

feature to redirect users to a malicious website and potentially causing them to fall victim to the phishing attempt (Broadhurst and Trivedi 2018).

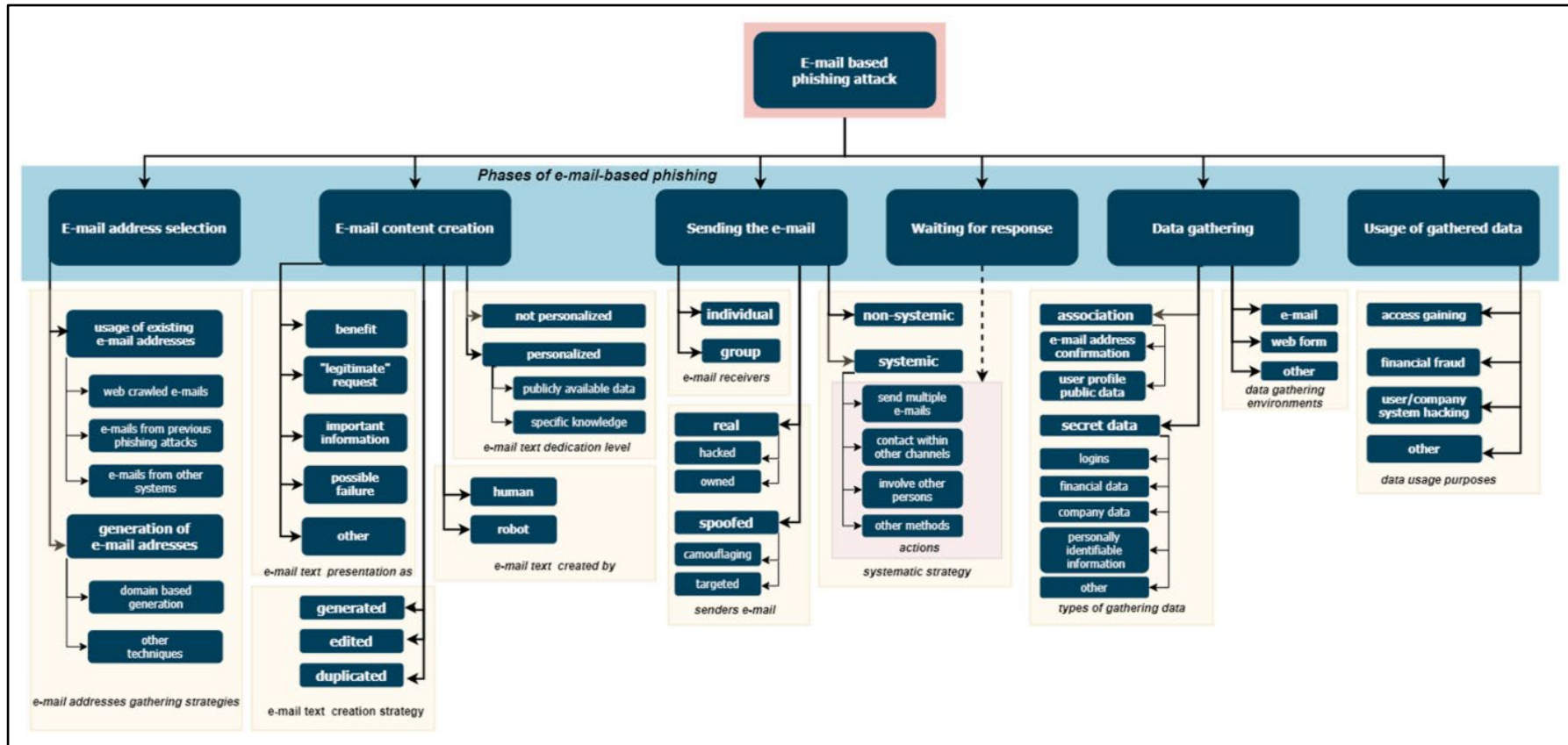


Figure 2.1 Phishing attack taxonomy adapted from (Almomani et al 2013, Rastenis et al. 2020)

Rastenis et al. (2020) developed a detailed taxonomy for email-based phishing attacks after analysing several existing taxonomies from published literature as per Figure 2.1. According to this research, there are six phases in email-based phishing attack:

1. Phase 1: Email address selection

Email address selection is one of the key elements in a phishing attack as there's no attack without an email address. There are two strategies in email address selection to obtain the potential victims email addresses. One is the usage of the existing email addresses. This strategy uses the existing email addresses, web crawled emails from Google search engine, as well as from open sources such as theHasverter and BeenVerified (Muhd Azi 2021), emails from previous phishing attacks, and emails from other systems.

The other strategy in this phase is generation of email addresses from domain-based generation and other techniques. Most organizations have their generic email addresses or distribution list such as, IT Service Desk, *pelajar*, or info. These types of emails are easier to guess and misused. Email addresses could also be generated using random sequence.

2. Phase 2: Email content creation

This phase has four strategies and involves in designing the email content. Victim engagement can be seen in how well the phishing email was designed.

First is how victims are engaged in the phishing attack. Ultimately, the victim has to believe that the email is legitimate.

- a. Benefit – Humans are always motivated by the benefit of something. The attacker promises a financial or other benefit to

motivate the victim to provide requested data. Often, the promised benefit is never delivered, while the data are used maliciously.

- b. Legitimate request – The phishing message appears legitimate and does not raise suspicion, leading the victim to automatically provide requested data without questioning its authenticity.
- c. Important information – The attacker creates a sense of urgency or an important event, causing stress for the victim. This stress may lead the victim to act quickly without carefully analyzing the email or verifying its authenticity.
- d. Possible failure – Similar to urgency, the attacker suggests that failure to provide the requested data will lead to negative consequences, such as system failure or loss of service. This strategy relies on understanding internal processes and the potential impact of not complying.
- e. Other - Phishing attacks can also exploit specific vulnerabilities or weaknesses of individual victims due to personalized or targeted content.

The second strategy is email text generation.

- a. Generated – A new phishing email is created from scratch.
- b. Edited – The email text is copied from another source, which could be a legitimate email or a previous phishing attack. Some parts, such as the recipient's name or specific details, are modified to suit the current attack.
- c. Duplicated – The email text is directly copied from existing sources without any modifications. This approach is quick but highly detectable.

The third strategy is email text creation.

- a. Human – The email text is manually written or modified by a person.
- b. Robot – The email text is generated or modified by a computer program or bot.

The fourth strategy is email personalization level.

- a. Personalised – The email text includes personalized information about the recipient. Spear phishing often uses personalised attacks.
- b. Not personalised – The email is generic and could be sent to anyone. It does not include any personal information about the recipient.

### 3. Phase 3: Sending the email

The method of sending phishing emails is also one of the important factor. One of the main indicators of phishing email is the sender's email address. The attackers may use their real or fake email address. Phishing emails can be sent individually or by a group (normally a distribution list).

### 4. Phase 4: Waiting for response

Once the phishing emails were sent, the attacker then just wait for the victim's response. However, sometimes the attacker would use some systematic strategies in order to get victim's response. This method involves multiple actions and requires knowledge about the victim to increase the attack's success probability.

- a. Sending multiple emails to the same victim, incorporating additional information or reminders in follow-up emails.

- b. Using other communication channels (phone calls, social networks, etc.) to remind and motivate the victim to act on the email.
- c. Involving another person to increase the credibility and urgency of the request.
- d. Publishing data in the media

#### 5. Phase 5: Data gathering

Data gathering is how the attacker collects the data.

- a. Email reply - The victim responds to the phishing email by providing the requested data.
- b. Webforms - The attacker creates a web page with data input functionality. These web pages can be unique or designed to mimic legitimate websites, tricking the user into submitting their data to the attacker.
- c. Other Methods - Attackers can also gather data using social networks, phone calls, or other channels.

#### 6. Phase 6: Usage of gathered data

- a. Gaining Access to Systems: If login credentials are obtained, they can be used to access systems belonging to the victim.
- b. Financial Fraud: The attack focuses on obtaining financial and personal data, leading the victim to transfer money to the attacker
- c. User/Company System Hacking: The attack gathers specific information about an enterprise's management structure, technologies, or other details, facilitating broader hacking efforts.



- d. Other Purposes: Various other purposes exist, which are less common and highly varied, so they are grouped into a general "other" category.

## **2.5 Effectiveness of Different Spear Phishing Campaigns**

In the research titled “Individual processing of phishing emails: How attention and elaboration protect against phishing” (Harrison et al 2016), was conducted with 194 participants from a university in the Northeastern US. Participants were exposed to phishing emails crafted with either fear-based or reward-based messages. Their responses were measured to evaluate susceptibility based on attention to email elements and elaboration of the phishing message. One of the hypotheses proposed in this research was, when it comes to information processing, fear-based phishing attacks are more effective compared to reward-based phishing attacks. Two types of phishing emails were designed in this study, one for fear-based phishing attack and the other for reward-based phishing attack. Fear-based phishing attacks phishing emails often contain urgent cues, such as "warning" or "deadline," to trigger fear and prompt immediate action (Harrison et al 2016). A fake Gmail email account (Gmail) was used to send the phishing emails.

A study conducted by Mousa (2022), explores the psychological and emotional aspects that make individuals susceptible to phishing attacks. Emotions are the key tool used by the threat actors. The paper investigated various emotional factors, such as trust, fear, and urgency, that phishers exploit to achieve their goals. People tend to share their information when strong emotions have been triggered. This paper also examines the role of security training and awareness programs in mitigating phishing attacks. It emphasizes the importance of educating individuals about different phishing techniques, recognizing suspicious emails, and adopting safe online practices.

## 2.6 Past Studies In UKM

Norhafizah Abu Bakar (2017) is the pioneer in developing spear phishing simulation in UKM. The spear-phishing simulation at UKM was a collaborative effort involving the Faculty of Information Science and Technology (FTSM), Information Technology Center, Bursary Department, and Department of Registrar. A total of 533 email addresses from five faculties were identified for the simulation, focusing on the topic of "Bantuan Kewangan 2016.". The sample included both science and technology (S&T) faculties, such as FTSM and the Faculty of Engineering and Built Environment (FKAB), and non-S&T faculties, such as the Faculty of Law (FUU), Faculty of Islamic Studies (FPI), and Faculty of Social Science and Humanities (FSSK).

Out of the 533 participants, 209 respondents (38%) entered their work ID (captured) and password (not captured). This included 95 respondents (45%) from S&T faculties and 103 respondents (49%) from non-S&T faculties. There wasn't a significant difference in the numbers which indicated both groups of staffs have concerning level of spear phishing awareness. Additionally, the analysis revealed that 140 respondents (67%) were from the management and professional group, while 69 respondents (33%) were from the operational group. The high response rate among the management and professional group further highlighted the urgent need for improved cybersecurity education.

In another research conducted in UKM by (Mohamad Alhaddad 2021), student's personality trait on spear susceptibility behaviour was studied. The study also explored the roles of IT background, gender, and age. Furthermore, the study evaluates the effectiveness of an embedded training system and examines whether message framing can enhance its effectiveness. Prior to the simulation, a personality trait survey was distributed to 100 participants. Following the survey, a real-life spear-phishing simulation was conducted to observe the participants' reactions and measure the influence of their personality traits on their susceptibility to phishing attacks.

Participants who fell victim to the phishing attempt by clicking on the malicious link were redirected to a training comic page designed to educate them about phishing tactics and prevention strategies. After a two-week period, a second round of spear-phishing emails was sent to the participants to measure the effectiveness of the training and assess whether different methods of message framing could further reduce the likelihood of phishing success.

Analysis of the data revealed that individuals with higher levels of anxiety are more likely to fall victim to spear-phishing emails. This finding underscores the importance of considering psychological factors when developing strategies to combat phishing attacks. It suggests that anxiety may impair an individual's ability to critically evaluate suspicious emails, making them more vulnerable to deception.

In addition to personality traits, the study also explored the impact of an embedded training program on reducing phishing susceptibility. The results were promising, indicating that the training program significantly reduced the click rate on spear-phishing emails among participants. This demonstrates that educational interventions can effectively enhance individuals' ability to recognize and avoid phishing attempts. However, when it came to message framing, the study did not find any significant impact on reducing phishing susceptibility.

## **2.7 Cybersecurity Awareness**

In this digital age, there are victims of online threats that occur regularly and are abused in a variety of ways. Previous research has revealed that university students are particularly vulnerable to internet threats and frauds. Cybersecurity knowledge should be prioritized across institutions rather than just in IT departments. As a result, university students must gain cybersecurity awareness to safeguard themselves and their data and assist in the creation of a safer digital environment.

The digital immersion and technological competence of university students characterize them. Despite their familiarity with technology, research reveals that they do not necessarily have great cybersecurity awareness (Moallem, 2019). The perceived vulnerability appears to be a key factor in shaping students' degrees of awareness. Those who feel they are more vulnerable are more worried about cybersecurity. Mai and Tick (2021) performed a survey among university students in Hungary and Vietnam to explore cyber security awareness and youth smartphone usage. Students from various nations and disciplines of study do not lack an understanding of cyber security; yet, they frequently overlook self-protection from online risks. Similarly, Gabra et al. (2020) concluded in a case study that cybersecurity awareness is not included in Nigerian tertiary institutions, implying that students lack cybersecurity education and understanding of phishing attacks.

As a result, increasing cybersecurity awareness among users, particularly university students, is critical. According to Mai and Tick (2021), formal cyber security education is critical since it can provide young users with an essential understanding of this worldwide issue as well as self-prevention from cyber risks. Furthermore, an integrated curriculum approach entails incorporating cybersecurity education within the core curriculum, ensuring that students from all disciplines gain basic knowledge. Furthermore, interactive and engaging awareness programs, such as workshops, seminars, and simulations, that include cyber security laws, risks, and prevention methods, help catch students' attention and give practical insights into cybersecurity dangers. Collaboration with industry specialists is recommended to give real-world viewpoints and bridge the gap between academic theory and practical implementation.

Combining behavioural psychology ideas into awareness efforts, on the other hand, has been found as an effective technique. Understanding the psychological factors that impact students' conduct enables the development of curricula that eliminate cognitive biases while simultaneously encouraging desirable cybersecurity practices. Subramaniam (2017) also proposed that instructors and administrators in educational

institutions have proper training to aid the younger generation in equipping for and combating the digital age struggle.

The importance of cybersecurity knowledge among university students cannot be stressed as technology evolves. This section investigated the varied nature of factors impacting awareness, the problems encountered, and the many solutions used to improve cybersecurity understanding. Future studies should concentrate on determining the efficacy of specific treatments as well as their long-term effects on students' cybersecurity practices. Finally, developing a cyber-resilient generation necessitates the collaboration of educational institutions, cybersecurity experts, and governments.

## **2.8 Summary**

Overall, this chapter explores into the university students' cybersecurity knowledge. It delves into the world of social engineering, cyber scam awareness, and numerous types of cyber dangers such as phishing attacks, hacking, investment scams, romance scams, and identity theft. The vulnerability of university students to online fraud, as well as their responses to internet fraud, are explored. Furthermore, the research examines core cybersecurity knowledge, identifying factors and obstacles impacting student awareness levels. The literature on cybersecurity awareness emphasizes the need for information distribution among university students. It promotes formal cybersecurity education as part of the curriculum, as well as engaging awareness programs and partnerships with industry professionals. The final portion emphasizes the ever-changing nature of technology as well as the critical role of cybersecurity knowledge in raising a cyber-resilient generation. It advocates for coordinated efforts among educational institutions, cybersecurity experts, and legislators to effectively manage the problems of the digital era.

## CHAPTER III

### METHODOLOGY

#### 3.1 Overview

Research methodology is paramount to ensure that the research can be carried out systematically and effectively in unravelling the research questions. The two main questions that this chapter focuses on are: how were the data gathered and how were they analysed? This chapter outlines the techniques, project flows, and strategies implemented in carrying out this study. To achieve the objectives of this research, this study is structured into four phases: research design, data collection, data analysis, and summarization.

This study employs a quantitative experimental research approach to investigate the susceptibility of UKM students to phishing attacks through simulated scenarios. Quantitative research warrants objectivity and dependability as no matter who conducts the research, the results should be replicated. It focuses on testing theories, establishing facts, illustrating how variables relate to one another, and conjecture the outcome (Van der Merwe 1996). Participants are chosen at random for the study population in an objective manner and statistical techniques are employed to test predetermined hypotheses about the relationship between variables.

Experimental research designed to determine cause-and-effect relationships between variables. It carries out the research in an objective, controlled manner to optimize precision and reach findings regarding a hypothesis statement (Bell 2009). Using this approach, one or more independent variables are manipulated and observed

on how those changes affect the dependent variables, all the while accounting for possible confounding variables. Randomization is used, and control and experimental groups are frequently included. The purpose is to ascertain whether changes in the independent variables cause observable changes in the dependent variables in order to establish causality.

In this study, the cause-and-effect relationship is examined through the manipulation of different types of spear phishing campaigns (cause) and how these different scenarios influence students' likelihood to fall for the phishing attempts.

1. Cause (Independent Variables): Different types of spear phishing campaigns (Job Scam, Password Reset, and COVID-19 survey).
2. Effect (Dependent Variables): The susceptibility of UKM students was measured by their response rates to these phishing emails (e.g., clicking on links, providing information).

There have been few spear phishing researches conducted by past UKM students which implements four phases are Planning, Research Design, Implementation, and Analysis (Smith 2010, Norhafizah Abu Bakar 2018, Ahmad Syukri Bin Abdullah 2019, Siti Zaleha Binti Ahmad 2020, Mohamad Alhaddad 2021, Muhd Azi Bin Peker 2021). This study adapts a similar methodology as the other studies, however, certain aspects in each phase, such as the target group, email template, email content, email tone have been modified to accommodate this study.

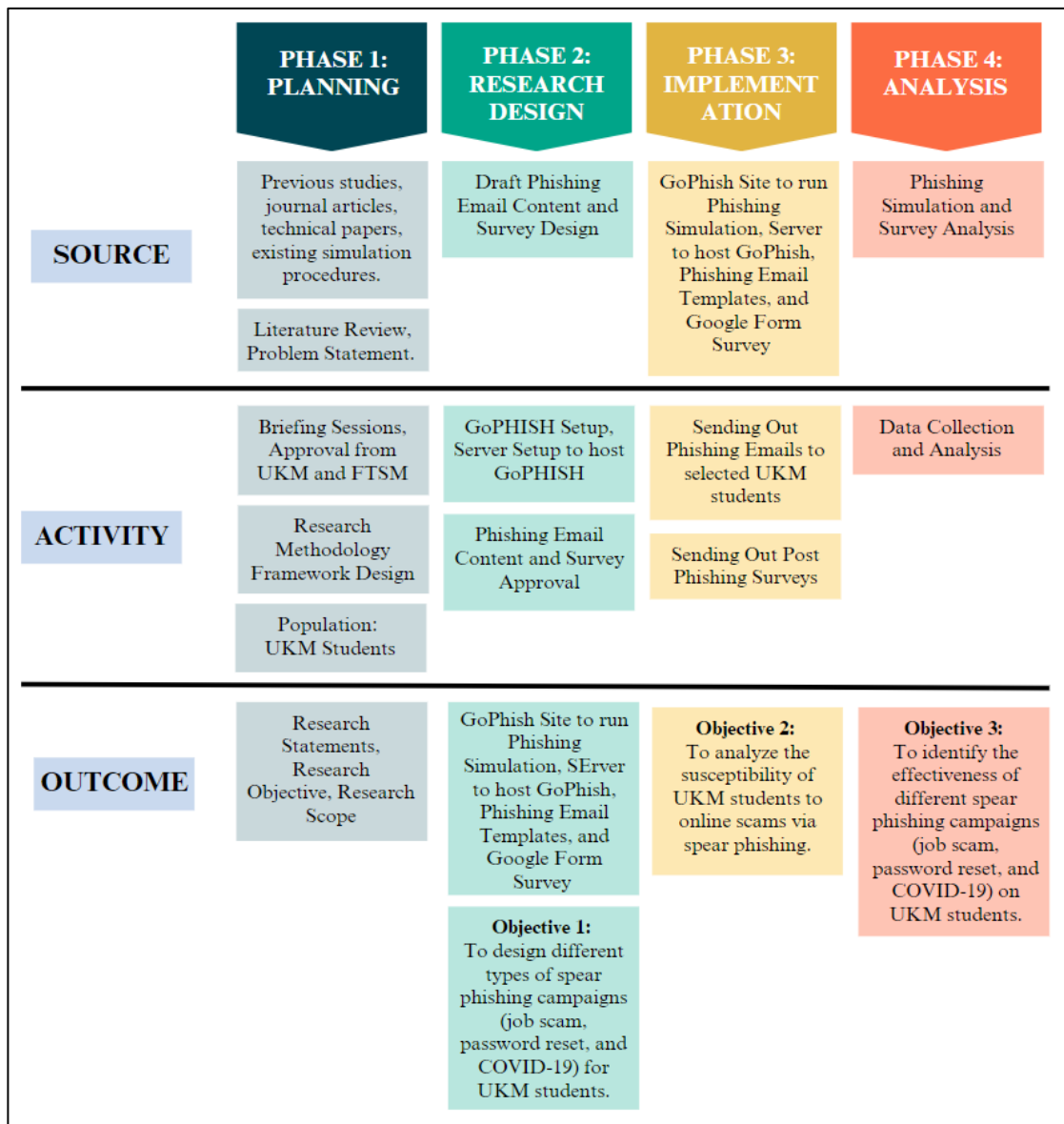


Figure 3.1 Research Methodological Framework (Adapted from Creswell 2014, Siti Zaleha Binti Ahmad 2020)

### 3.2 Phase 1: Planning

In the preliminary phase of this research, a detailed literature review (Chapter II) was conducted to understand current findings and gaps related to phishing susceptibility among students. Based on the studies, problem statement, research questions, and research objectives are formulated, as outlined in Chapter I (Introduction).



In addition, this phase also involved in outlining the scope of the research, including the types of phishing campaigns to be tested (job scams, password resets, and COVID-19). Necessary study instruments, such as the email templates for the phishing campaigns and the metrics for evaluating student responses are determined as well. Ethical considerations are paramount in any research. Approval from management was obtained to a ensure seamless study. During the discussion, the objective, scope, methodology, and target audiences of the phishing campaign were presented.

### 3.2.1 Target Group

The sample of UKM students selected for this study was determined using a random number generation method. This approach was facilitated by the fact that students' email addresses at UKM are derived from their matriculation numbers, making it easy to generate and guess potential email addresses. As such, the students' demographic information such as their gender, faculty, and age were undetermined. The randomly generated email addresses were grouped in three with approximately 250 students in each group. However, since the email addresses were random guesses, some of the email addresses were non-existent.

Table 3.1 Sample Size

<b>Target Group</b>	<b>Size</b>
GROUP 1	253
GROUP 2	254
GROUP 3	255

### 3.3 Phase 2: Research Design

In this phase Objective 1 for this study, which was to design different types of spear phishing campaigns (Job Scam, Password Reset, and COVID-19 survey) for UKM students was implemented. Email topic and content, technical preparations, and survey design were focused. There were three types of phishing simulation that represented positive campaign (Job Scam), negative campaign (Password Reset), and neutral campaign (COVID-19 survey) were designed for this study. Although many phishing attacks are reward-based like the Nigerian scams that promise financial rewards in exchange for personal information, fear-based phishing attacks like imminent account closure or compromised accounts are also prominent.

These topics were chosen due to their high relevance and potential to deceive. Key factors included in designing the email content are the relevance of the topic to the target audience, realism of the email content, authenticity, and professional language. It is also crucial to identify indicators that can signal to the students that the emails and the websites might be suspicious.

In addition, the required metrics for data collection were also identified and set. These metrics serve as quantitative measures for data analysis. The metrics include the number of students who opened the email, number of students who clicked on the link, and number of students who submitted their data on the fake site. These data were collected using GoPhish, an open-source phishing simulation platform. Both the emails and the website were developed with subtle but obvious red flags to indicate that they were suspicious.

Table 3.2 Red Flag Indicator Table

Category	Title	Description
Email	PELUANG PEKERJAAN SAMBIL MASA UNTUK PELAJAR UKM DI PUSAT PENDAFTAR UKM	<ol style="list-style-type: none"> <li>1. Email was sent from a Gmail address: Official email will always be sent from legitimate UKM address.</li> <li>2. Sense of urgency: The email created a sense of urgency by implying that the opportunity is limited and requires immediate action.</li> <li>3. Hidden link: Suspicious and mismatched URLs</li> <li>4. Too good to be true: The offer seems too good to be true, with promises of high pay for minimal work.</li> <li>5. Nonexistence department: There's no "Pejabat Admin Pendaftar" in UKM.</li> </ol>
Email	Urgent: Security Breach - Password Reset Required	<ol style="list-style-type: none"> <li>1. Email was sent from a Gmail address: Official email will always be sent from legitimate UKM address</li> <li>2. Sense of urgency: The email created a sense of urgency for security concerns.</li> <li>3. Hidden link: Suspicious and mismatched URLs</li> <li>4. Nonexistence department: There's no "Pejabat Admin Pendaftar" in UKM.</li> </ol>
Email	Urgent: COVID-19 Vaccination Survey for Campus Safety	<ol style="list-style-type: none"> <li>1. Email was sent from a Gmail address: Official email will always be sent from legitimate UKM address.</li> <li>2. Hidden link: Suspicious and mismatched URLs</li> <li>3. Nonexistence department: There's no "Pejabat Admin Pendaftar" in UKM.</li> </ol>
Fake Website	UKM Login Page	<ol style="list-style-type: none"> <li>1. Unsecure Connection: Website uses http instead of https</li> </ol>

to be continued...

...continuation

2. Mismatched URL: URL did not match UKM domain and used IP address.  
<http://3.26.172.37/?rid=ExcsiX9>
- 

### 3.3.1 Positive Phishing Campaign: Job Scam

The email title for Job Scam phishing simulation was “PELUANG PEKERJAAN SAMBIL MASA UNTUK PELAJAR UKM DI PUSAT PENDAFTAR UKM” which translates to “Part-Time Job Opportunities For UKM Students At The UKM Registration Center”. The job opportunity was to work virtually as the registrar's admin assistant for RM250 per week. This is an absurdly high salary for a part-time position. The content was designed in such a way to catch the attention of students seeking extra money.

To add credibility, the email included professional language and contact information supposedly linked to the university. To create a sense of urgency, the email urged students to apply immediately by clicking on a provided link as there was a deadline for the job offer.

Table 3.3 Job Scam Email Design

Parameter	Description
Email Subject	PELUANG PEKERJAAN SAMBIL MASA UNTUK PELAJAR UKM DI PUSAT PENDAFTAR UKM
Sender	pusatpendaftarukm@gmail.com
Email Tone	Positive – The job scam email created a positive feeling among students by promising an attractive amount of money for a part-time position.

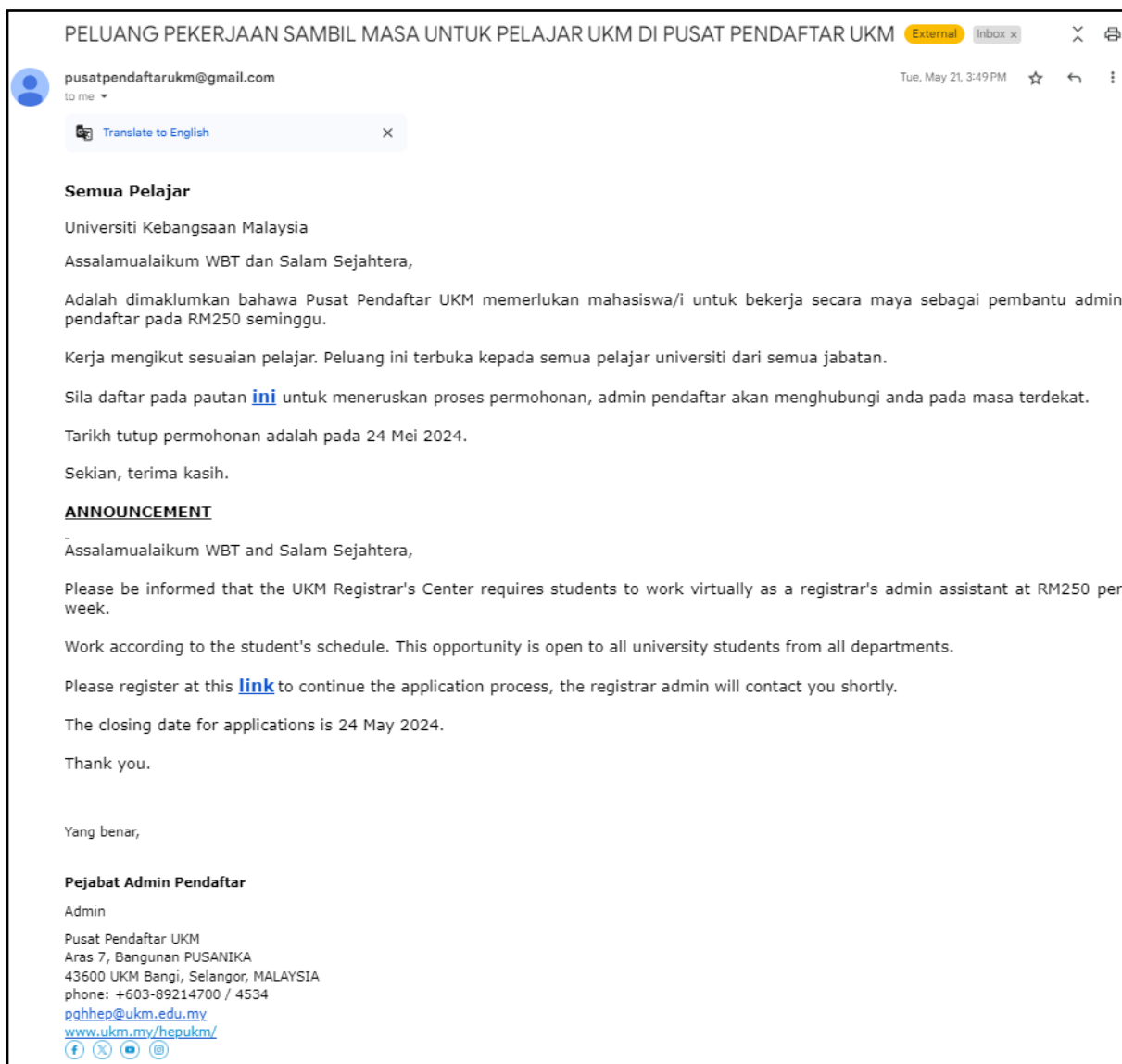


Figure 3.2 Job Scam Phishing Email

### 3.3.2 Negative Phishing Campaign: Urgent: Security Breach - Password Reset Required

The email title for password reset phishing simulation was “Urgent: Security Breach - Password Reset Required”. This email was designed to mimic a legitimate security alert from the university, warning students of a potential security breach and urging them to reset their passwords immediately. Therefore, detailed instructions for creating strong passwords were provided. The email employed a sense of urgency and concern for security.

Table 3.4 Password Reset Email Design

Parameter	Description
Email Subject	Urgent: Security Breach - Password Reset Required
Sender	<a href="mailto:pusatpendaftarukm@gmail.com">pusatpendaftarukm@gmail.com</a>
Email Tone	Negative – The email induces fear among students by urging and claiming that there is a potential security breach and requesting immediate action.

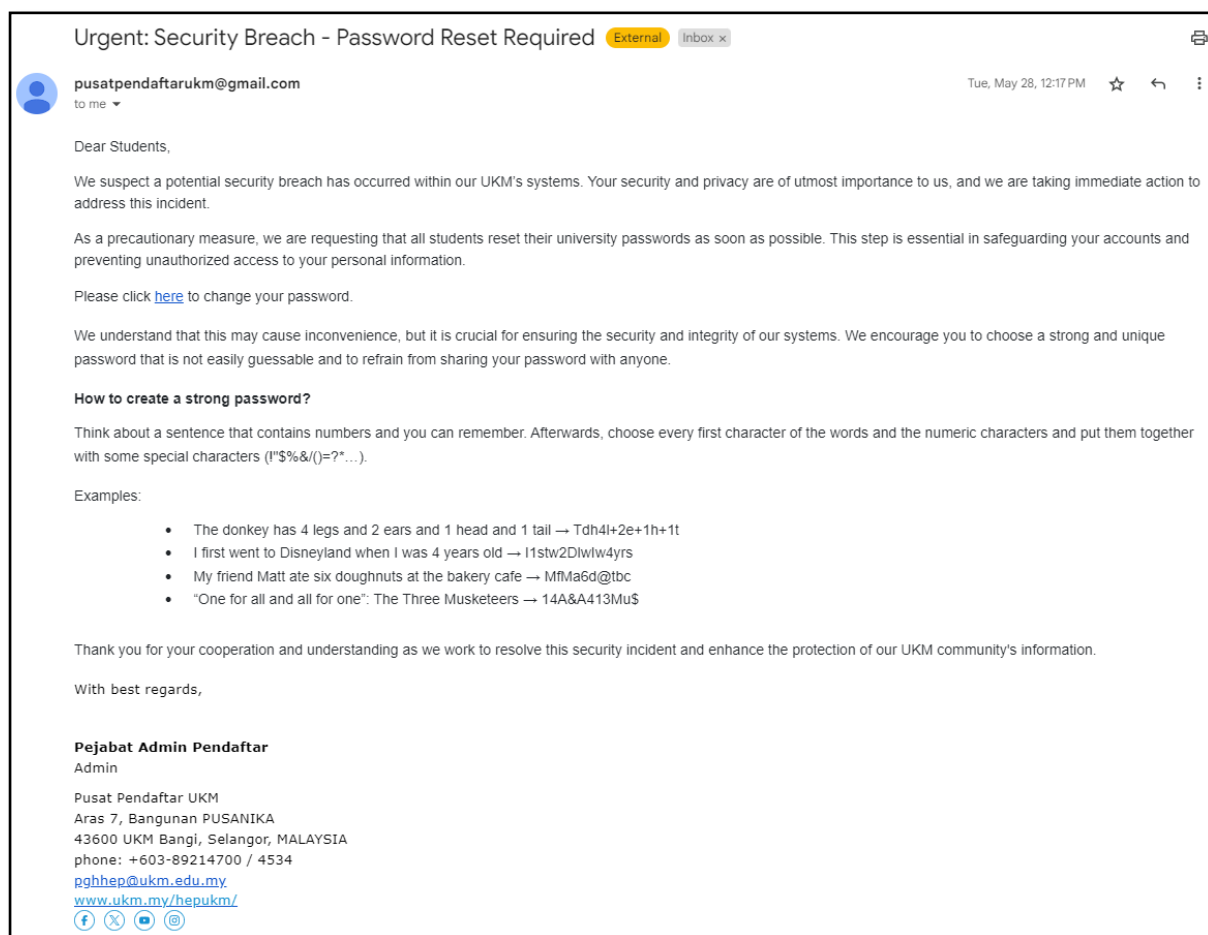


Figure 3.3 Password Reset Phishing Email

### 3.3.3 Neutral Phishing Campaign: Urgent: COVID-19 Vaccination Survey for Campus Safety

The email title for COVID-19 Survey phishing simulation was “Urgent: COVID-19 Vaccination Survey for Campus Safety”. This email was crafted to appear as an official communication from the university's administration. It emphasized the health and safety

of UKM students by referencing recent COVID-19 cases on campus. The email maintained an informational and factual tone by requesting students to participate in a survey to gather information about their vaccination status.

Table 3.5 COVID-19 Survey Email Design

Parameter	Description
Email Subject	Urgent: COVID-19 Vaccination Survey for Campus Safety
Sender	<a href="mailto:pusatpendaftarukm@gmail.com">pusatpendaftarukm@gmail.com</a>
Email Tone	Neutral – The email was informational and did not imply any consequences for students who chose not to participate in the survey.

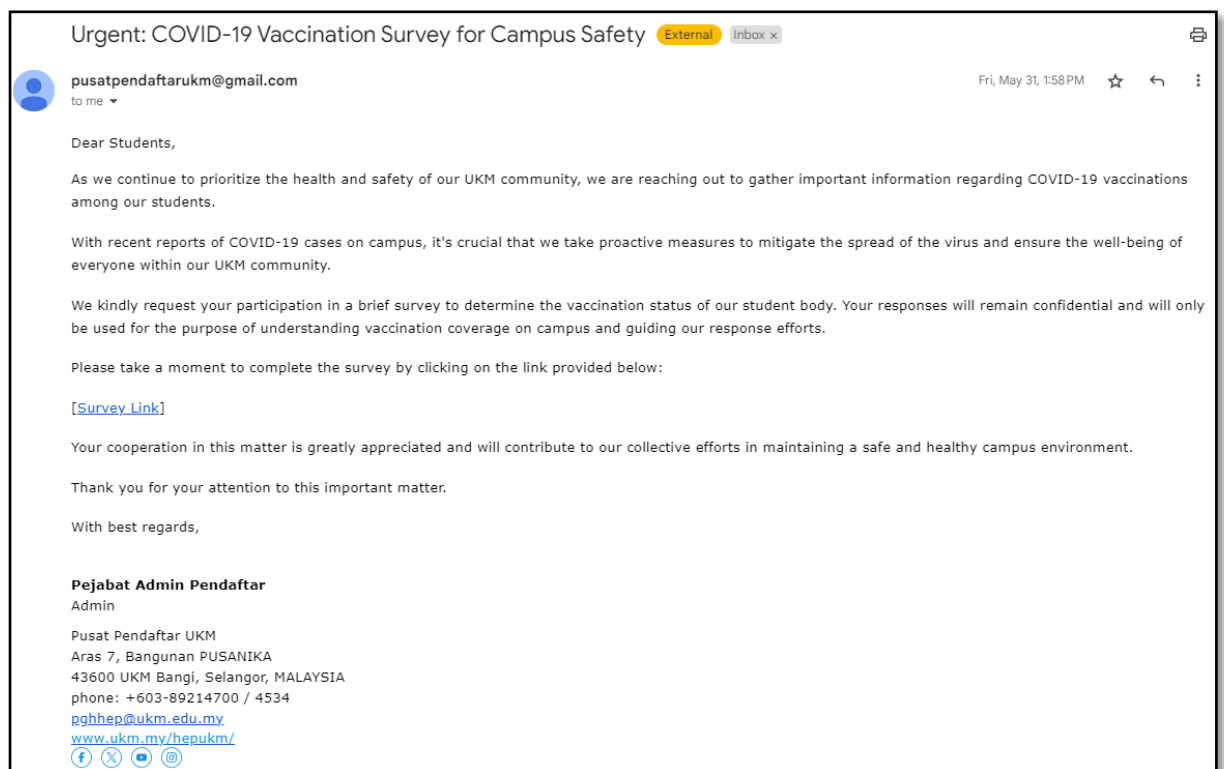


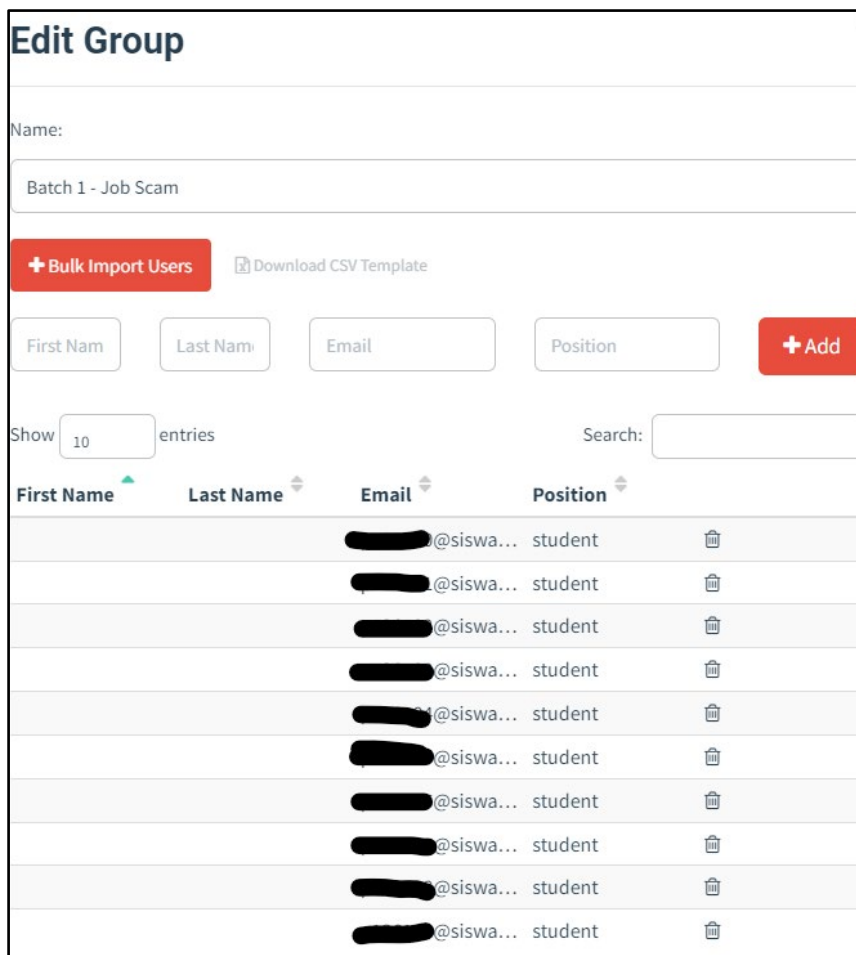
Figure 3.4 COVID-19 Survey Phishing Email

### 3.3.4 Phishing Simulation Design

#### 3.3.4.1 GoPhish

The phishing campaigns in this research were launched using GoPhish platform. Several things need to be configured before the phishing campaigns can be launched.

1. User Group – Three user groups were created on the GoPhish platform, corresponding to the three different groups of students. Each student group was added to a specific user group to track the results seamlessly.



**Edit Group**

Name:

[+ Bulk Import Users](#) [Download CSV Template](#)

[+ Add](#)

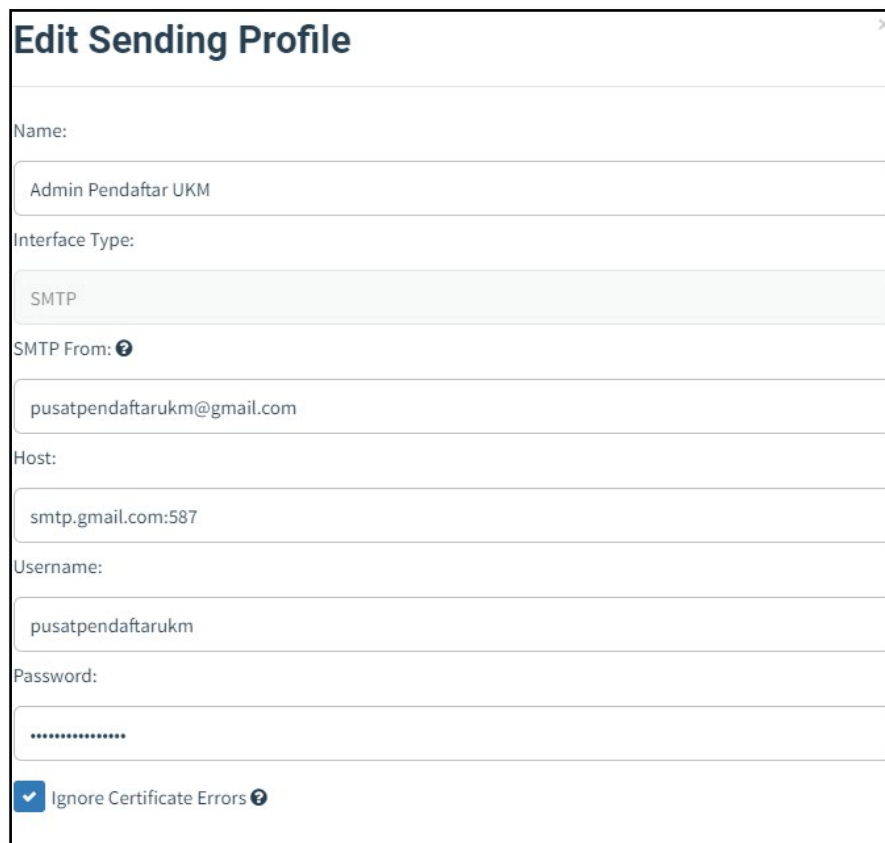
Show  entries Search:

First Name	Last Name	Email	Position	
		████████@siswa...	student	
		████████@siswa...	student	
		████████@siswa...	student	
		████████@siswa...	student	
		████████@siswa...	student	
		████████@siswa...	student	
		████████@siswa...	student	
		████████@siswa...	student	
		████████@siswa...	student	
		████████@siswa...	student	

Figure 3.5 GoPhish User Group Creation



2. Sending Profile – A new Gmail account, *pusatpendaftarukm@gmail.com* was created to mimic an email that appears to be from UKM.



**Edit Sending Profile**

Name:  
Admin Pendaftar UKM

Interface Type:  
SMTP

SMTP From: ⓘ  
pusatpendaftarukm@gmail.com

Host:  
smtp.gmail.com:587

Username:  
pusatpendaftarukm

Password:  
.....

Ignore Certificate Errors ⓘ

Figure 3.6 GoPhish Sending profile

3. Landing Page – The landing page was created by importing the existing, legitimate UKM login page. The password capture option was disabled to not capture and store student's credentials. Once data was submitted on the fake UKM login page, the site will redirect to a Google Form to collect the demographic information of the students.

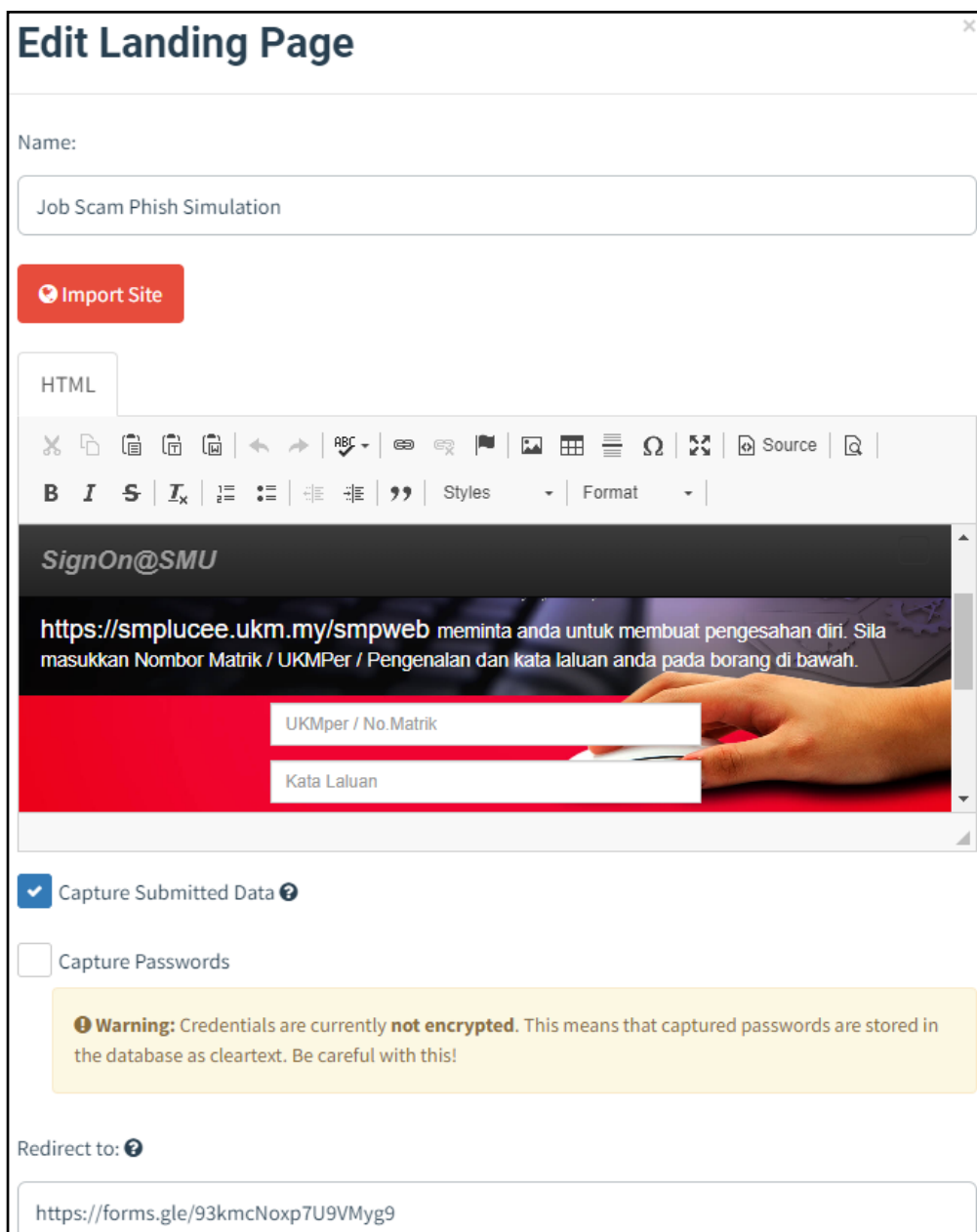


Figure 3.7 GoPhish Landing Page

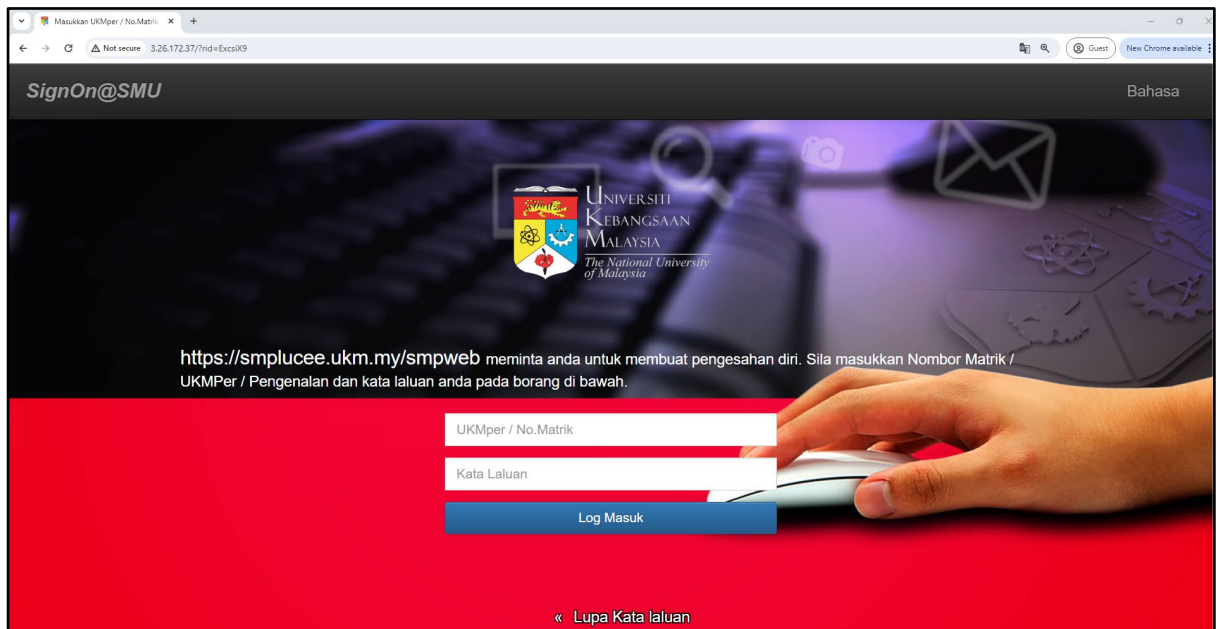


Figure 3.8 Fake UKM Landing Page

## PELUANG PEKERJAAN SAMBILAN UNTUK PELAJAR UKM DI PUSAT PENDAFTAR UKM

Terima kasih kerana mengambil bahagian dalam tinjauan ini. Privasi anda adalah penting bagi kami dan semua jawapan tinjauan akan dirahsiakan.

Thank you for participating in this survey. Your privacy is important to us and all survey responses will be kept confidential.

p111939@siswa.ukm.edu.my [Switch account](#)

\* Indicates required question

Email \*

Record p111939@siswa.ukm.edu.my as the email to be included with my response

Jantina / Sex \*

Lelaki / Male

Perempuan / Female

Figure 3.9 Google Form Redirection

4. Email Template – Three email templates were created to be sent. Although the envelope sender was put as [pghhep@ukm.edu.my](mailto:pghhep@ukm.edu.my), it was still showing the Gmail address in the email due to email setting by UKM.

## Edit Template

Name:

Envelope Sender: ?

Subject:

Text  HTML

\*Semua Pelajar\*

Universiti Kebangsaan Malaysia

Assalamualaikum WBT dan Salam Sejahtera,

Adalah dimaklumkan bahawa Pusat Pendaftar UKM memerlukan mahasiswa/i untuk  
bekerja secara maya sebagai pembantu admin pendaftar pada RM250 seminggu.

Add Tracking Image

Figure 3.10 GoPhish Job Scam Email Template

## Edit Template ✕

Name:

Envelope Sender: ?

Subject:

Dear Students,

We are reaching out to you today with urgent information regarding a potential security breach that has recently occurred within our UKM's systems. Your security and privacy are of utmost importance to us, and we are taking immediate action to address this incident.

As a precautionary measure, we are requesting that all students reset their university passwords as soon as possible. This step is essential in safeguarding your accounts and preventing unauthorized access to your personal information.

Add Tracking Image

Figure 3.11 GoPhish Password Reset Email Template



### 3.3.4.2 Amazon EC2

In order to host the GoPhish platform, a server must be set up. This was done using virtual servers (instances) on Amazon Elastic Compute Cloud EC2 (Amazon EC2). Amazon Elastic Compute Cloud EC2 (Amazon EC2) is a web service provided by Amazon Web Services (AWS) that offers resizable computing capacity in the cloud. The server setup involved configuring the EC2 instance with the required security groups, ensuring that it was secure and accessible only to authorized personnel.

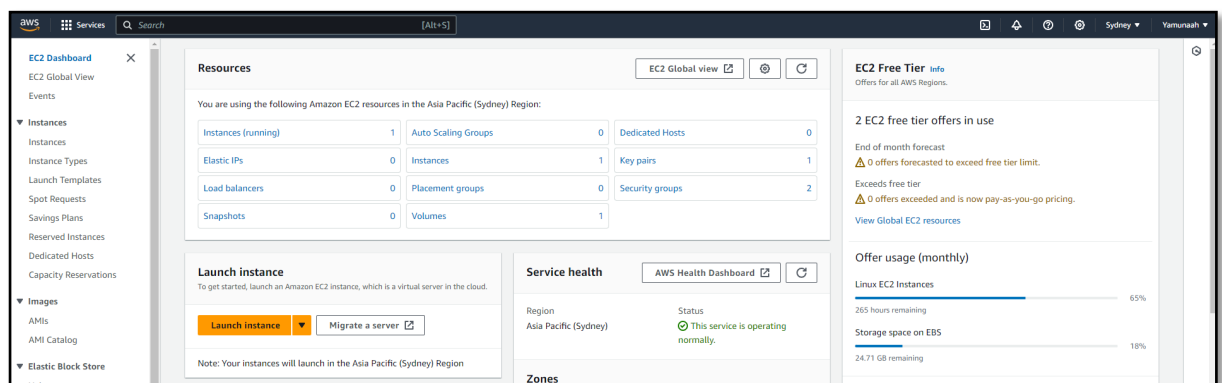


Figure 3.13 AWS EC2 Dashboard

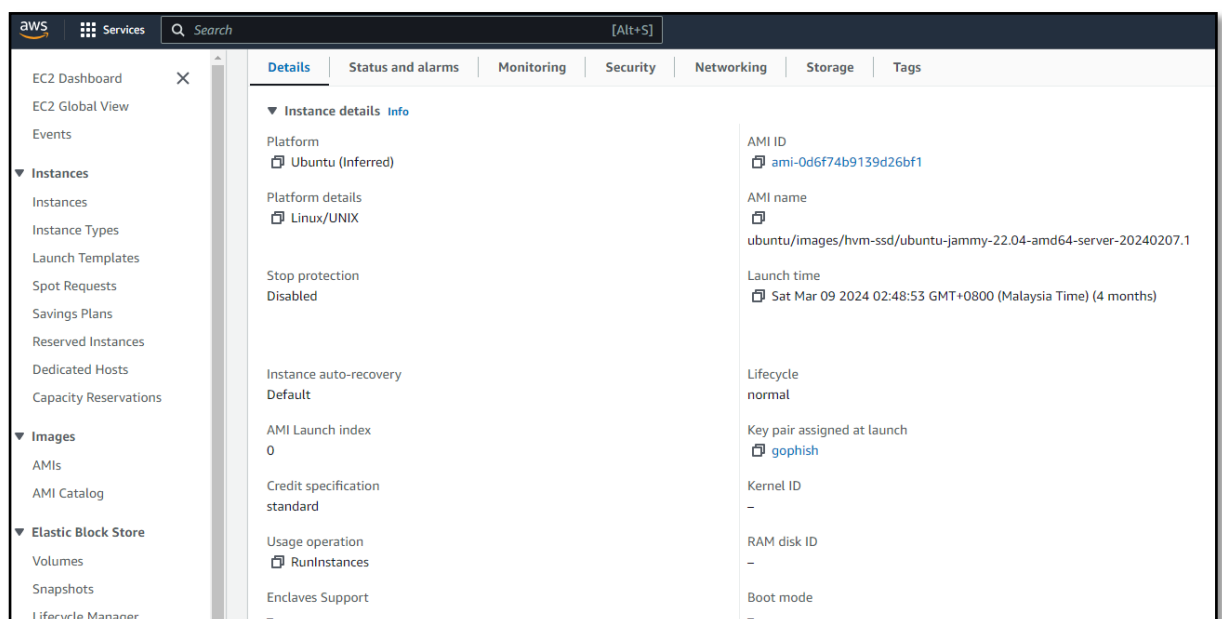


Figure 3.14 AWS EC2 Instance Details

```

(X11: Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.49 Safari/537.36""
time="2024-06-21T13:31:55Z" level=info msg="43.131.59.56 - - [21/Jun/2024:13:31:55 +0000] \"/GET /webroot/phpinfo.php HTTP/1.1\" 404 19 \"\" \"Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.49 Safari/537.36""
time="2024-06-21T13:32:02Z" level=info msg="43.131.59.56 - - [21/Jun/2024:13:32:02 +0000] \"/GET / HTTP/1.1\" 404 19 \"\" \"Mozilla/5.0 (X11; Linux x86_64
) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.49 Safari/537.36""
time="2024-06-21T13:32:03Z" level=info msg="43.131.59.56 - - [21/Jun/2024:13:32:03 +0000] \"/POST / HTTP/1.1\" 404 19 \"\" \"Mozilla/5.0 (X11; Linux x86_6
4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.49 Safari/537.36""
2024/06/21 13:32:27 http: TLS handshake error from 60.52.151.219:2089: remote error: tls: unknown certificate
2024/06/21 13:34:27 http: TLS handshake error from 60.52.151.219:2179: remote error: tls: unknown certificate
2024/06/21 13:36:27 http: TLS handshake error from 60.52.151.219:2266: remote error: tls: unknown certificate
2024/06/21 13:37:27 http: TLS handshake error from 60.52.151.219:2321: remote error: tls: unknown certificate
2024/06/21 13:39:27 http: TLS handshake error from 60.52.151.219:2424: remote error: tls: unknown certificate
2024/06/21 13:41:27 http: TLS handshake error from 60.52.151.219:2510: remote error: tls: unknown certificate
2024/06/21 13:42:27 http: TLS handshake error from 60.52.151.219:2563: remote error: tls: unknown certificate
2024/06/21 13:44:27 http: TLS handshake error from 60.52.151.219:2672: remote error: tls: unknown certificate
2024/06/21 13:45:27 http: TLS handshake error from 60.52.151.219:2722: remote error: tls: unknown certificate
2024/06/21 13:46:27 http: TLS handshake error from 60.52.151.219:2768: remote error: tls: unknown certificate
time="2024-06-21T13:48:12Z" level=info msg="185.254.196.173 - - [21/Jun/2024:13:48:12 +0000] \"/GET /.env HTTP/1.1\" 404 19 \"\" \"Mozilla/5.0 (X11; Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36""
time="2024-06-21T13:48:13Z" level=info msg="185.254.196.173 - - [21/Jun/2024:13:48:13 +0000] \"/POST / HTTP/1.1\" 404 19 \"\" \"Mozilla/5.0 (X11; Linux x8
6_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36""
2024/06/21 13:48:27 http: TLS handshake error from 60.52.151.219:2862: remote error: tls: unknown certificate
2024/06/21 13:49:27 http: TLS handshake error from 60.52.151.219:2913: remote error: tls: unknown certificate
2024/06/21 13:51:27 http: TLS handshake error from 60.52.151.219:3015: remote error: tls: unknown certificate
2024/06/21 13:53:27 http: TLS handshake error from 60.52.151.219:3134: remote error: tls: unknown certificate
2024/06/21 13:54:27 http: TLS handshake error from 60.52.151.219:3208: remote error: tls: unknown certificate
2024/06/21 13:55:27 http: TLS handshake error from 60.52.151.219:3257: remote error: tls: unknown certificate
2024/06/21 13:57:27 http: TLS handshake error from 60.52.151.219:3362: remote error: tls: unknown certificate
2024/06/21 13:58:27 http: TLS handshake error from 60.52.151.219:3412: remote error: tls: unknown certificate
2024/06/21 14:08:27 http: TLS handshake error from 60.52.151.219:3551: remote error: tls: unknown certificate
2024/06/21 14:01:27 http: TLS handshake error from 60.52.151.219:3601: remote error: tls: unknown certificate
time="2024-06-21T14:02:10Z" level=info msg="135.125.244.48 - - [21/Jun/2024:14:02:10 +0000] \"/GET /.env HTTP/1.1\" 404 19 \"\" \"Mozilla/5.0 (X11; Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36""
time="2024-06-21T14:02:10Z" level=info msg="135.125.244.48 - - [21/Jun/2024:14:02:10 +0000] \"/POST / HTTP/1.1\" 404 19 \"\" \"Mozilla/5.0 (X11; Linux x86
64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36""
2024/06/21 14:02:27 http: TLS handshake error from 60.52.151.219:3742: remote error: tls: unknown certificate
2024/06/21 14:04:27 http: TLS handshake error from 60.52.151.219:3979: remote error: tls: unknown certificate
2024/06/21 14:06:27 http: TLS handshake error from 60.52.151.219:4097: remote error: tls: unknown certificate
2024/06/21 14:07:27 http: TLS handshake error from 60.52.151.219:4162: remote error: tls: unknown certificate
2024/06/21 14:08:27 http: TLS handshake error from 60.52.151.219:4217: remote error: tls: unknown certificate
2024/06/21 14:09:27 http: TLS handshake error from 60.52.151.219:4270: remote error: tls: unknown certificate
2024/06/21 14:11:27 http: TLS handshake error from 60.52.151.219:4372: remote error: tls: unknown certificate
time="2024-06-21T14:11:41Z" level=info msg="20.117.180.87 - - [21/Jun/2024:14:11:41 +0000] \"/GET / HTTP/1.1\" 404 19 \"\" \"python-requests/2.32.3\"""
ubuntu@ip-172-31-46-14:~$ 2024/06/21 14:13:27 http: TLS handshake error from 60.52.151.219:4530: remote error: tls: unknown certificate

```

Figure 3.15 GoPhish Server Host (Ubuntu)

### 3.3.5 Post Simulation Survey Design

After students submitted their data through the fake UKM login page, they will be redirected to a Google Form to collect their demographic information. The questionnaires as presented in APPENDIX A1, APPENDIX A2, and APPENDIX A3 were limited to only demographic information in order to not alert the students. As each group of students will go through three rounds of phishing simulations, it was not revealed that the link they clicked was part of a phishing simulation.

Once all rounds of phishing campaigns for all three groups of students were completed, one post simulation survey was sent to all three groups of students to gather feedback and insights regarding this phishing campaign. A total of 762 emails were sent including to the no response addresses.



**PELUANG PEKERJAAN SAMBILAN UNTUK PELAJAR UKM DI PUSAT PENDAFTAR UKM**

**B** *I* U

Terima kasih kerana mengambil bahagian dalam tinjauan ini. Privasi anda adalah penting bagi kami dan semua jawapan tinjauan akan dirahsiakan.

Thank you for participating in this survey. Your privacy is important to us and all survey responses will be kept confidential.

This form is automatically collecting emails from all respondents. [Change settings](#)

Figure 3.16 Job Scam Google Form

**Student Survey**

**B** *I* U

We want to provide clarification and assure you that this was part of a planned phishing simulation exercise conducted internally.

Your data and personal information were never at risk during this simulation, and there has been no actual security breach within our systems. Your accounts and information remain secure, and there is no need to reset your password at this time.

Thank you for participating in this survey. Your privacy is important to us and all survey responses will be kept confidential.

This form is automatically collecting emails from all respondents. [Change settings](#)

Figure 3.17 Password Reset Google Form

**COVID-19 Vaccination Survey for Campus Safety**

**B** *I* U

Terima kasih kerana mengambil bahagian dalam tinjauan ini. Privasi anda adalah penting bagi kami dan semua jawapan tinjauan akan dirahsiakan.

Thank you for participating in this survey. Your privacy is important to us and all survey responses will be kept confidential.

This form is automatically collecting emails from all respondents. [Change settings](#)

Figure 3.18 COVID-19 Survey Google Form

The post simulation survey was also designed using Google Form. This survey aimed to assess participants' awareness of phishing threats, their experiences during the simulation, and their responses to the phishing emails received. There were 16 questions to this survey as presented in APPENDIX B. Demographic information was asked for as well since the information wasn't available.

Dear All,

You are receiving this email as you were one of the students who received the below phishing simulation email:

" PELUANG PEKERJAAN SAMBIL MASA UNTUK PELAJAR UKM DI PUSAT PENDAFTAR UKM"  
" Urgent: Security Breach - Password Reset Required"  
" Urgent: COVID-19 Vaccination Survey for Campus Safety"

The phishing emails you received were part of my Master's research. They were designed to mimic real phishing attempts to measure awareness and response. **Rest assured, no personal information or passwords were captured during this simulation. The study was conducted in a secure environment to ensure your privacy and data protection.**

Please take a few minutes to complete a short post-simulation survey.

Your feedback is invaluable and will help to gain deeper insights into the effectiveness of the phishing scenarios and the overall awareness of phishing threats among students.

[[Survey Link](#)]

Your cooperation in this matter is greatly appreciated.

Thank you.

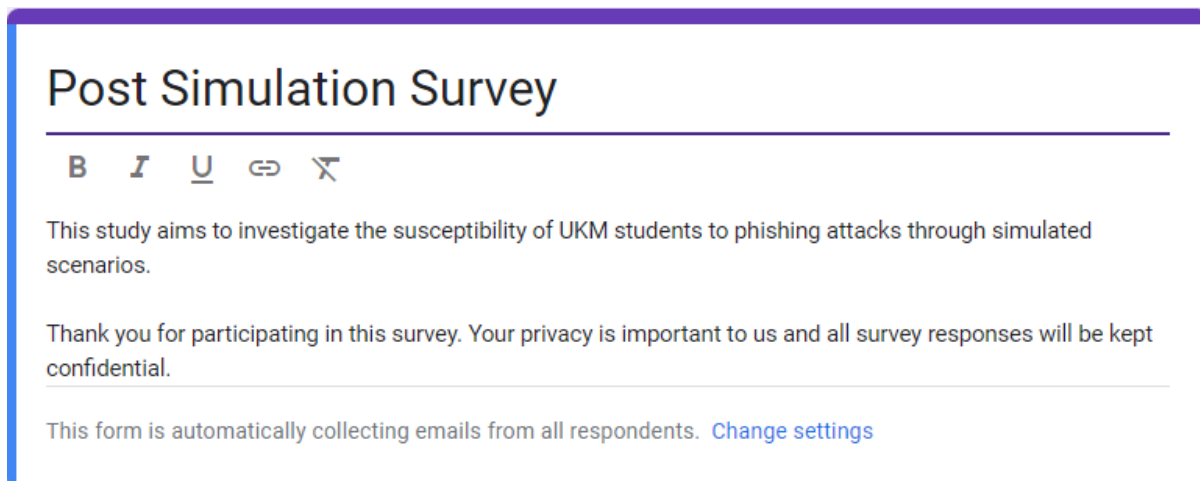
Any questions can be directed to:

Name: Yamunaah Rani Ravichanthar

Program: Master of Cyber Security (Faculty of Information Science and Technology)

Email: [P111939@siswa.ukm.edu.my](mailto:P111939@siswa.ukm.edu.my)

Figure 3.19 Post Simulation Email



The image shows a screenshot of a Google Form titled "Post Simulation Survey". The form has a white background with a blue border. At the top, the title "Post Simulation Survey" is displayed in a large, bold, black font. Below the title, there is a horizontal line. Underneath the line, there are five icons: a bold 'B', an italic 'I', an underlined 'U', a link icon, and a crossed-out 'X'. The main body of the form contains three paragraphs of text. The first paragraph states: "This study aims to investigate the susceptibility of UKM students to phishing attacks through simulated scenarios." The second paragraph says: "Thank you for participating in this survey. Your privacy is important to us and all survey responses will be kept confidential." The third paragraph reads: "This form is automatically collecting emails from all respondents. [Change settings](#)".

Figure 3.20 Post Simulation Google Form

### 3.4 Phase 3: Implementation

Objective 2 of this research which was to analyse the susceptibility of UKM students to online scams via spear phishing was applied in implementation phase. In this phase, the execution of phishing campaigns and the distribution of the post simulation survey was encompassed.

During one of the discussions, a real-time demonstration was conducted to illustrate the flow of the phishing simulation. The phishing campaign was launched in waves for different groups with intervals of a few days to weeks in between. Throughout the campaign, the metrics were collected to measure the success rates of each phishing attempt, such as the number of clicks on phishing links and the submission of personal data. The post simulation survey was shared with the students who opened the emails after the completion of all rounds of phishing campaigns.

Table 3.6 Implementation Timeline

<b>Date</b>	<b>Activity</b>
19 <sup>th</sup> Jan 2024	Early discussion with TPM about the phishing campaign and real time demonstration of the simulation.
13 <sup>th</sup> Mar 2024	Job Scam Phishing Campaign for Group 1
15 <sup>th</sup> May 2024	COVID-19 Phishing Campaign for Group 2
15 <sup>th</sup> May 2024	Password Reset Phishing Campaign for Group 3
16 <sup>th</sup> May 2024	COVID-19 Phishing Campaign for Group 1
21 <sup>st</sup> May 2024	Job Scam Phishing Campaign for Group 2
21 <sup>st</sup> May 2024	Job Scam Phishing Campaign for Group 3
24 <sup>th</sup> May 2024	Password Reset Phishing Campaign for Group 1
28 <sup>th</sup> May 2024	Password Reset Phishing Campaign for Group 2
31 <sup>st</sup> May 2024	COVID-19 Phishing Campaign for Group 3
3 <sup>rd</sup> June 2024	Post simulation survey email was sent.

### **3.5 Phase 4: Data Analysis**

The data analysis phase of this study involved a detailed examination of the collected data to evaluate the effectiveness of the phishing campaigns and understand the susceptibility of UKM students to various types of phishing attacks. Objective 3, to identify the effectiveness of different spear phishing campaigns (job scam, password reset, and COVID-19) on UKM students was accomplished in this phase.

Quantitative data from the GoPhish platform was analyzed to determine the click-through rates and the number of students who submitted personal information in response to each phishing email. This data was further segmented by campaign type—job scam, password reset, and COVID-19 survey—to identify which type of phishing attempt was most effective. Additionally, the post-simulation survey responses were analyzed to assess students' awareness and perceptions of phishing threats.

### 3.6 Summary

This chapter outlines the methodology used to conduct phishing simulations, data collection, and data analysis. There were three types of phishing campaigns, Job Scam, Password Reset, and COVID-19 survey were conducted for three groups of students involving 601 students. Three groups of students were selected to ensure each type of phishing campaign, Job Scam, Password Reset, and COVID-19 survey could be tested independently and comparatively among different groups, allowing for a clear assessment of each campaign's effectiveness.

These phishing emails were sent out to the three student groups in waves with no particular order and totalled nine phishing simulations. All three topics were selected to be relatable and realistic for the students. Following the completion of all phishing campaigns, a post-simulation survey was distributed to the participants.

## CHAPTER IV

### RESULTS AND DISCUSSION

#### 4.1 Introduction

Chapter IV delves into the results and discussion derived from the phishing campaigns and post simulation survey that had been conducted on UKM students. This chapter highlights the effectiveness of the phishing campaigns in terms of success rates and students' susceptibility to falling for such attacks. It also analyses the feedback gathered from the post simulation survey to understand students' awareness and knowledge about phishing threats.

Three groups of students were randomly selected for the study using their matriculation IDs. Each group was exposed to a different set of phishing email first, distributed in a randomized order. This approach aimed to investigate whether the type of phishing email received first had any impact on the students' engagement rate. Group 1 received Job Scam email first, followed by COVID-19 and Password Reset emails. Group 2 received COVID-19 email, followed by Job Scam email, and then Password Reset email. On the other hand, Group 3 received Password Reset first, and then Job Scam email, and followed by COVID-19.

### 4.1.1 Job Scam Phishing Simulation Data Analysis

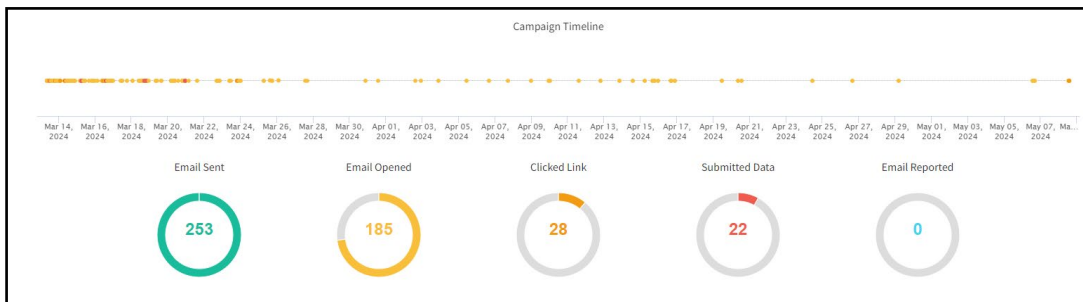


Figure 4.1 Group 1 Job Scam Phishing Simulation Result from GoPhish

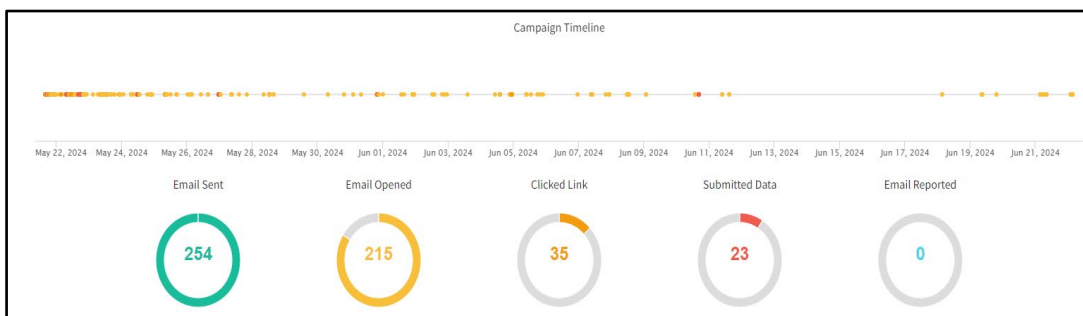


Figure 4.2 Group 2 Job Scam Phishing Simulation Result from GoPhish

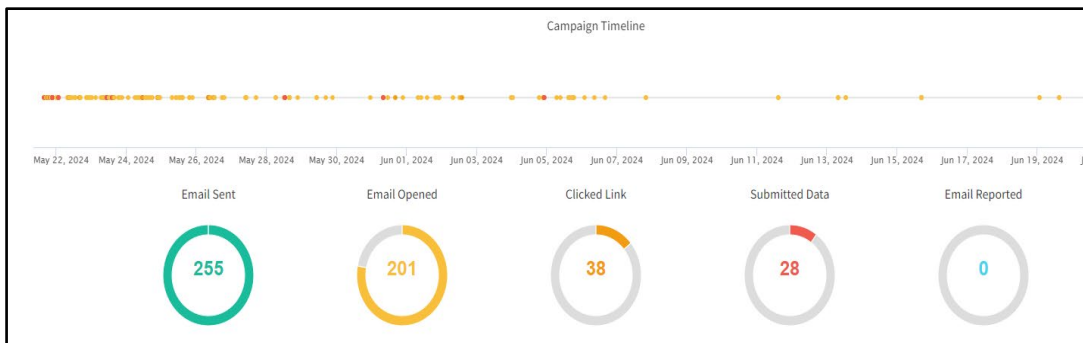


Figure 4.3 Group 3 Job Scam Phishing Simulation Result from GoPhish

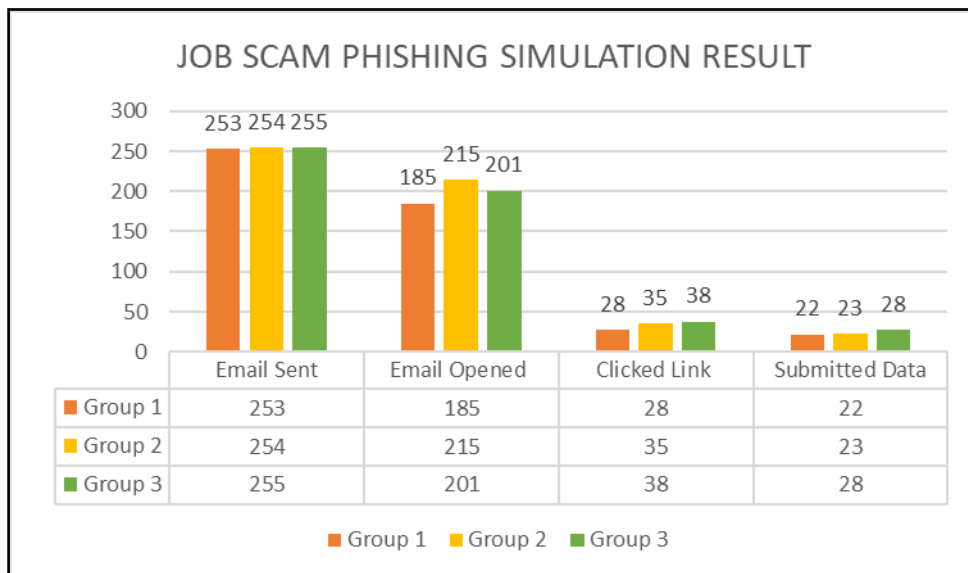


Figure 4.4 Job Scam Phishing Simulation Result

Figure 4.1, Figure 4.2, and Figure 4.3 show the results from GoPhish platform dashboard of students who opened the emails, clicked the links, and submitted their data on the fake UKM login page. Some of the emails sent were left unopened. This could potentially be due to the email being nonexistent or the student deleting it without opening.

From Figure 4.4, for Group 1's phishing simulation, 185 emails were opened out of 253 sent emails which was 73.12%. 28 students (15.14%) clicked on the email link, while 22 students (11.89%) submitted their data. Whereas, for Group 2, 215 emails (84.65%) were opened out of 254, 35 students (16.28%) clicked on the link, and 23 students (10.70%) submitted their data. For Group 3, 255 emails were sent, out of which 201 students (78.82%) opened the email, 38 (18.90%) students clicked on the link, and 28 (13.93%) students submitted their credentials. Group 3 had the highest click rate and data submitted.



#### 4.1.2 Password Reset Phishing Simulation Data Analysis

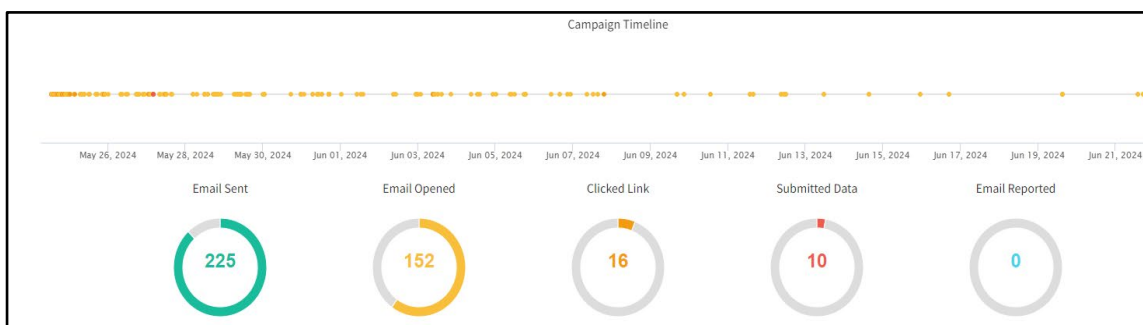


Figure 4.5 Group 1 Password Reset Phishing Simulation Result from GoPhish

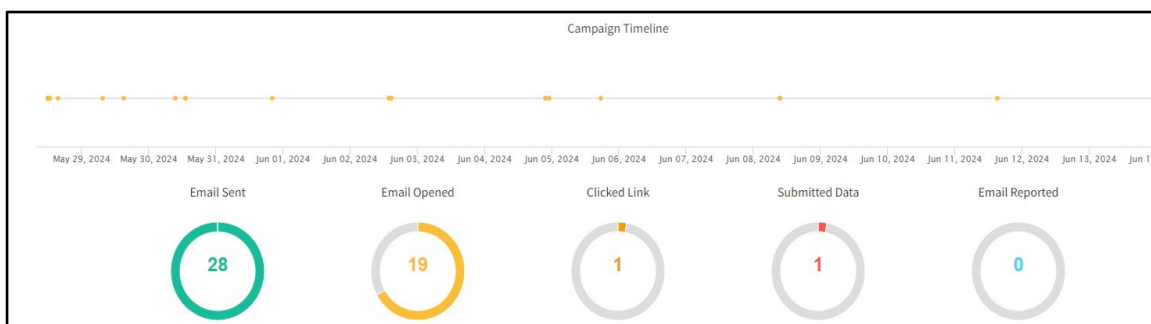


Figure 4.6 Group 1 Password Reset Phishing Simulation Result from GoPhish 2.0

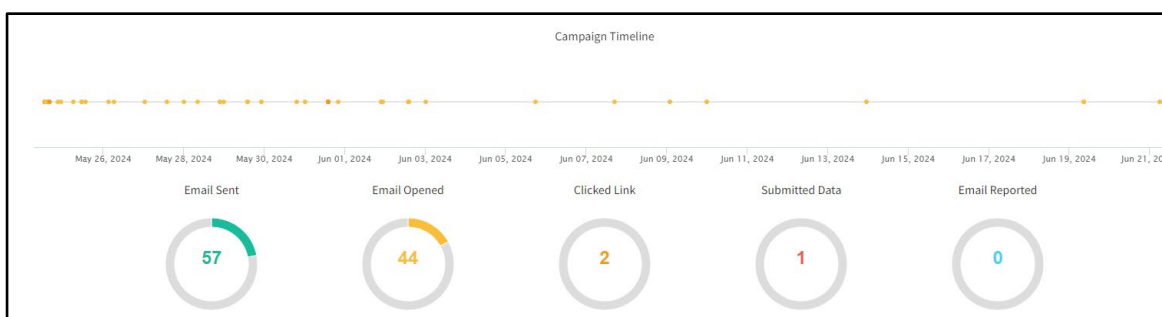


Figure 4.7 Group 2 Password Reset Phishing Simulation Result from GoPhish

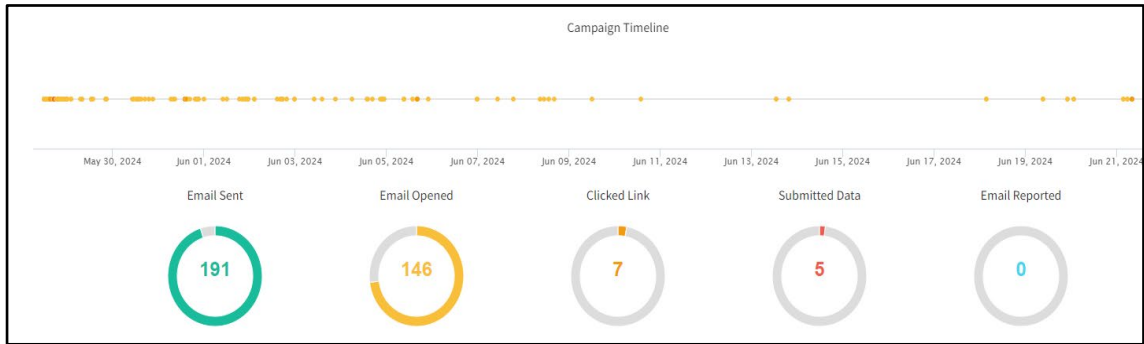


Figure 4.8 Group 2 Password Reset Phishing Simulation Result from GoPhish 2.0

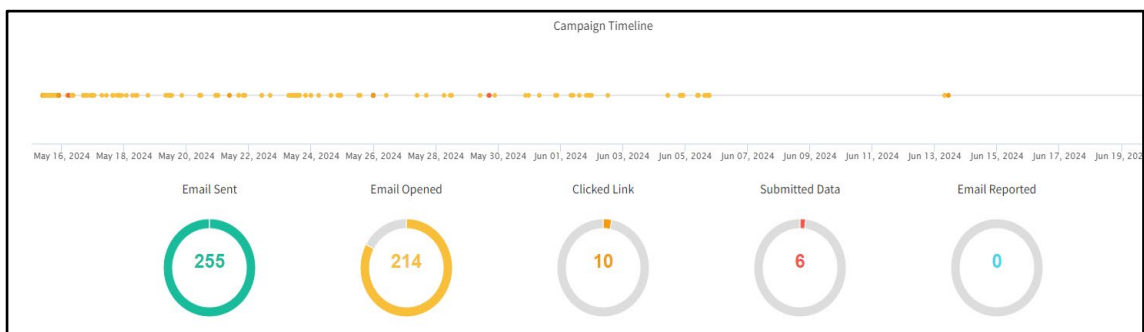


Figure 4.9 Group 3 Password Reset Phishing Simulation Result from GoPhish 2.0

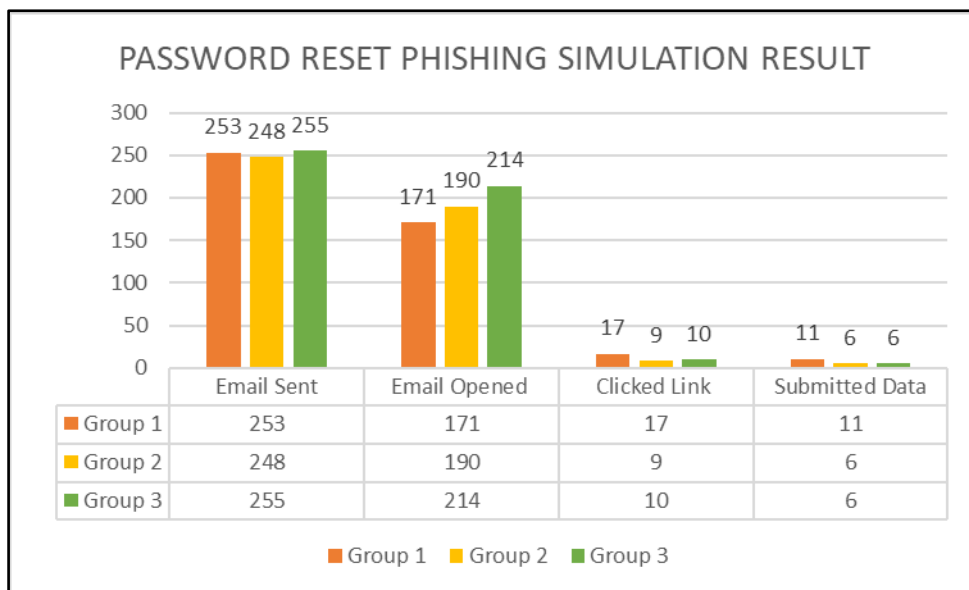


Figure 4.10 Password Reset Phishing Simulation Result

Figure 4.5, Figure 4.6, Figure 4.7, Figure 4.8, and Figure 4.9 show the results for number of students who opened the emails, clicked the links, and submitted their data for Password Reset phishing simulations on GoPhish platform. Some of the emails sent during the phishing simulations of Group 1 and Group 2 were not sent due to server error. Emails were sent separately in another simulation for the errored emails.

Group 1 has the highest success rate for link clicked 17 (9.94%) and submitted data 11 (6.43%) despite having the lowest rate for email opened, which was 171 (67.59%) out of 253 emails sent. During Group 2's Password Reset phishing simulation, out of 248 emails sent, 190 students (76.61%) opened the email, 9 students (4.74%) clicked on the link, and 6 students (3.16%) submitted their data. Meanwhile, 214 students (83.92%) opened the email out of 255 sent emails, 10 students (4.67%) clicked on the link, and six students (2.80%) submitted their data for Group 3.

#### 4.1.3 Covid-19 Survey Phishing Simulation Data Analysis

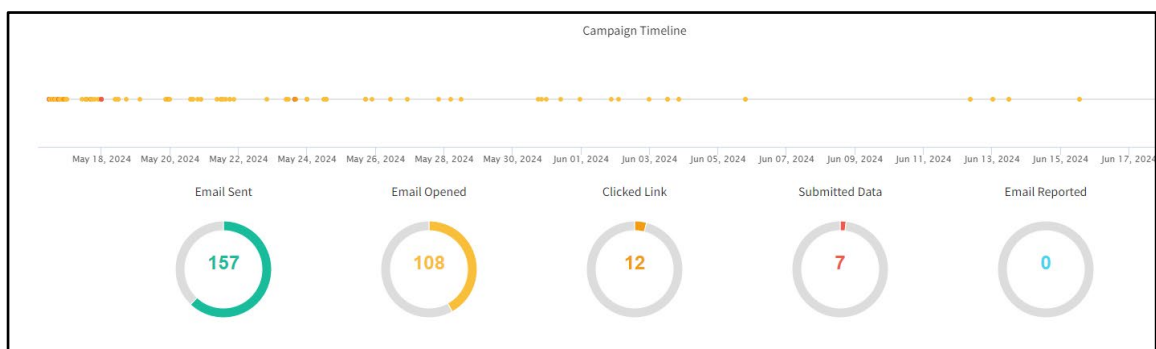


Figure 4.11 Group 1 COVID-19 Survey Phishing Simulation Result from GoPhish

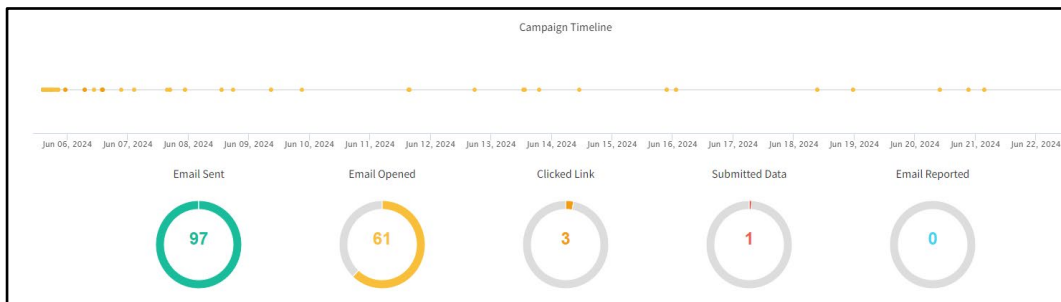


Figure 4.12 Group 1 COVID-19 Survey Phishing Simulation Result from GoPhish 2.0

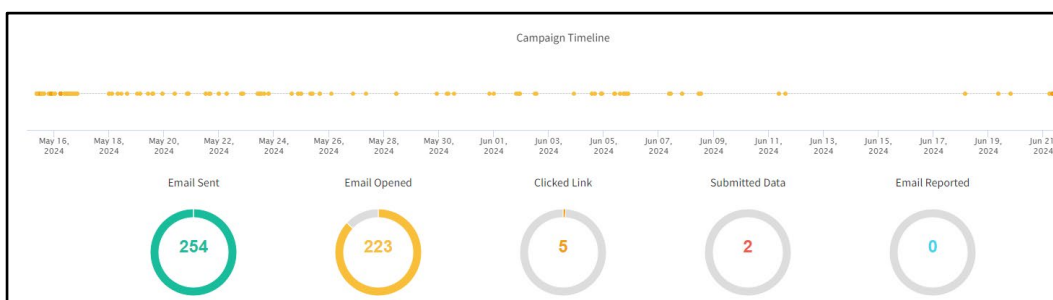


Figure 4.13 Group 2 COVID-19 Survey Phishing Simulation Result from GoPhish

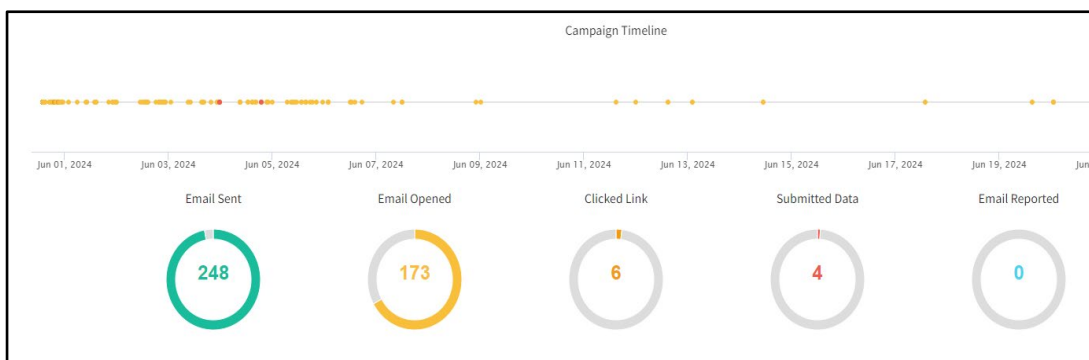


Figure 4.14 Group 3 COVID-19 Survey Phishing Simulation Result from GoPhish

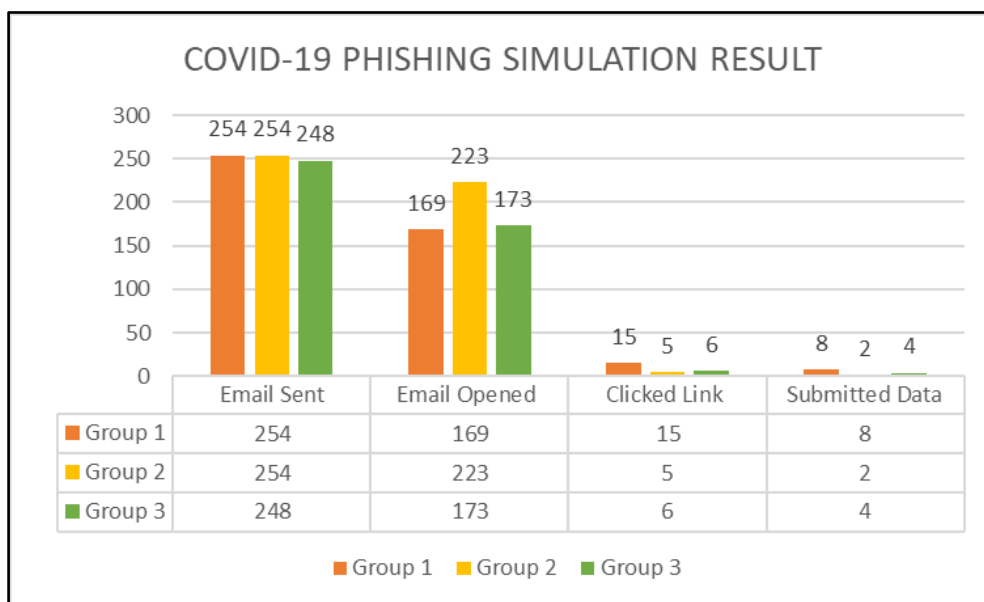


Figure 4.15 COVID-19 Survey Phishing Simulation Result

Figure 4.11, Figure 4.12, Figure 4.13, and Figure 4.14 present the results for COVID-19 Survey phishing simulations on GoPhish platform for the number of students who opened the emails, clicked the links, and submitted their data. A few of the emails sent during Group 1 phishing simulations were not sent due to server error. A separate simulation was conducted for the errored emails. Figure 4.15 shows the COVID-19 Survey Phishing Simulation Result from GoPhish dashboard.

In Group 1, 169 students (66.54%) opened the email, 15 students (8.88%) clicked on the link, and 8 students (4.73%) submitted their data. During the phishing simulation of Group 2, 223 students (87.80%) opened the email out of 254 emails sent. However, only five students (2.24%) clicked the link and 2 students (0.90%) submitted their data. For Group 3, 248 emails were sent out. 173 students (69.76%) opened the email, six students (3.47%) clicked on the link, and four students (2.31%) shared their data.

## 4.2 Demographic Data Analysis

The demographic information of the students who submitted their credentials were collected through a Google Form questionnaire that was redirected from the fake UKM login page.

### 4.2.1 Gender

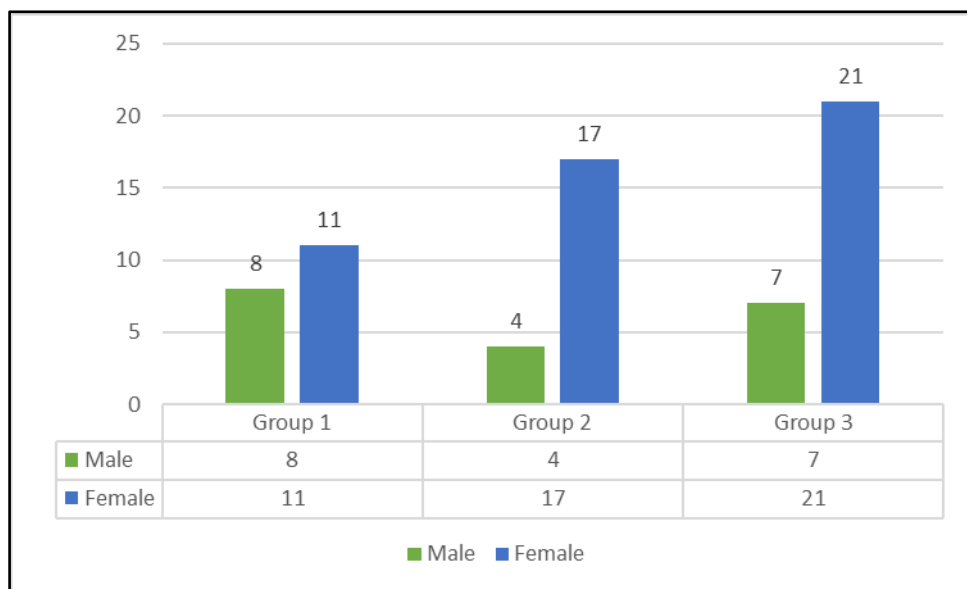


Figure 4.16 Job Scam Phishing Simulation Result by Gender

The first demographic analysis of the student groups was by gender. The above chart for Job Scam phishing simulation gender classification shows that female students' response rate was significantly higher compared to male students across all three phishing campaigns. 11 female students (57.89%) submitted their data during Job Scam phishing simulation, 17 students (80.95%) submitted during Password Reset phishing simulation, and 21 students (75.00%) submitted during COVID-19 phishing simulation. Meanwhile, eight male students (42.11%) submitted their data during Job Scam phishing simulation, four students (19.05%) submitted during Password Reset phishing simulation, and seven students (25.00%) submitted during COVID-19 phishing simulation.

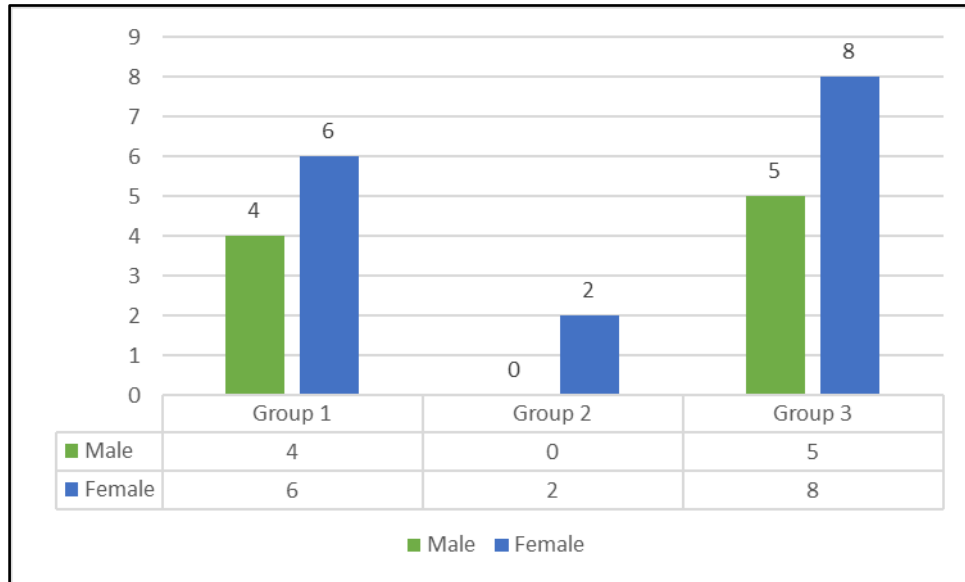


Figure 4.17 Password Reset Phishing Simulation Result by Gender

Figure 4.17 shows gender classification for Password Reset phishing simulation. Response rate of female students of all three groups for this campaign were higher compared to male students as well. Six female students (60.00%) submitted their data during Job Scam phishing simulation, two students (100.00%) submitted during Password Reset phishing simulation, and eight students (61.54%) submitted during COVID-19 phishing simulation. Whereas only four male students (40.00%) submitted their data during Job Scam phishing simulation and five male students (38.46%) submitted during COVID-19 phishing simulation. There was no response from male students from Group 2 for this phishing simulation.

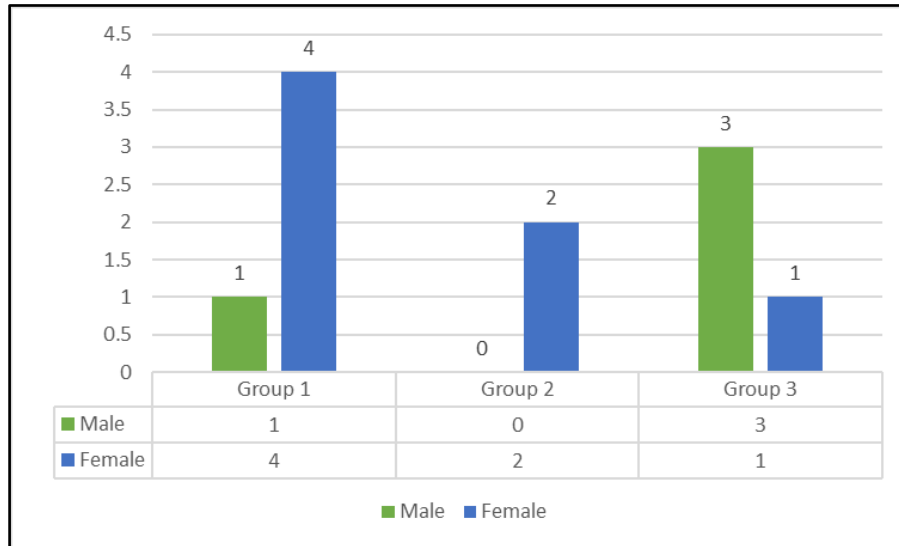


Figure 4.18 COVID-19 Survey Phishing Simulation Result by Gender

The gender classification results for COVID-19 phishing campaign were slightly different from the previous two campaigns. The results were mixed with female students' response rate were higher for Group 1 and Group 2 and male students response rate was higher in Group 3. For Group 1, four female students (80.00%) responded and only one male student (20.00%) responded. For Group 2, no male students responded and two female students (100.00) responded, and for Group 3, three male students (75.00%) responded and only one female student (25.00%).



## 4.2.2 Age

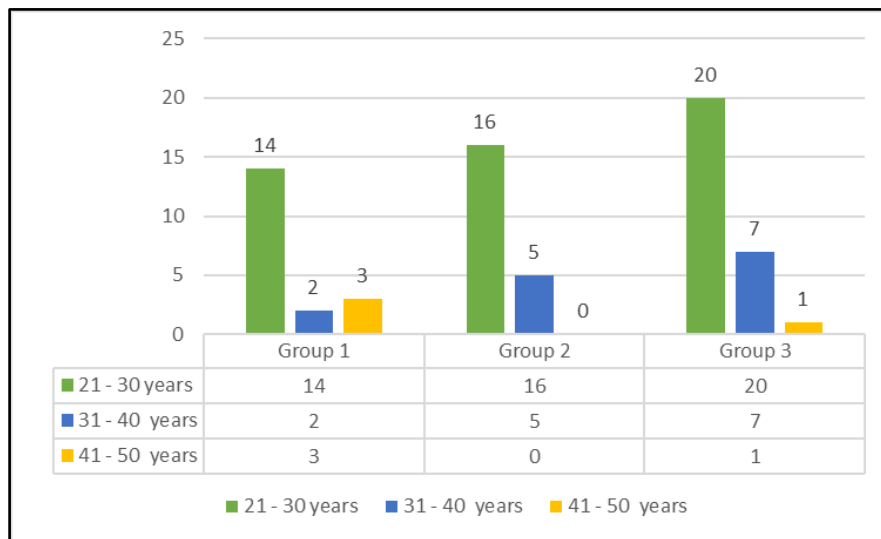


Figure 4.19 Job Scam Phishing Simulation Result by Age

The second demographic analysis of the student groups was by gender. Students aged between 21-30 years had the highest response rate among all three groups. For Group 1, 14 students (73.68%) were aged between 21-30 years old, two students (10.53%) were aged between 31-40 years old, and three students (15.79%) were aged between 41- 50 years old. For Group 2, 16 students (76.19%) were aged between 21-30 years old and five students (23.81%) aged between 31-40 years old. Group 3 students had the highest data submission rate with 20 students (71.43%) aged between 21-30 years old, seven students (25.00%) were aged between 31-40 years old, and only one student (3.57%) was aged between 41- 50 years old.

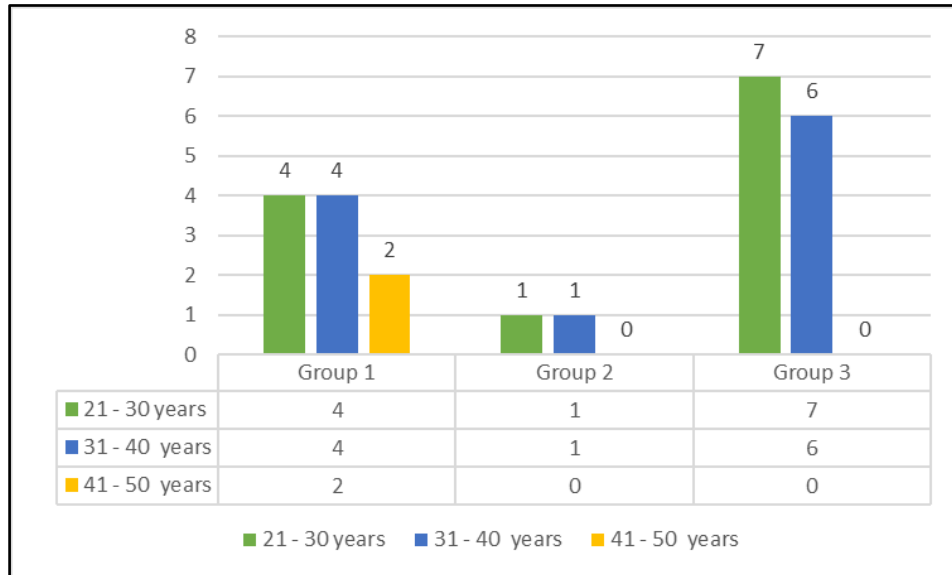


Figure 4.20 Password Reset Phishing Simulation Result by Age

For Group 1 Password Reset Phishing Simulation, both 21-30 years old and 31-40 years old age categories had four students (40.00%) submit their data and two students (20.00%) were aged between 41-50 years old. For Group 2, both 21-30 years old and 31-40 years old age categories only had one student (50.00%) each that had submitted their data. While for Group 3, seven students (53.85%) were aged between 21-30 years old and six students (46.15%) were aged between 31-40 years old.

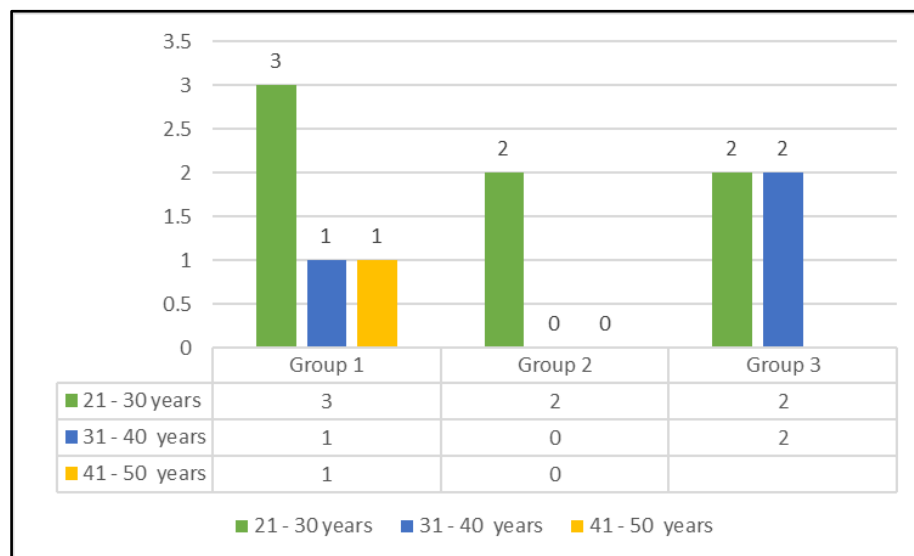


Figure 4.21 COVID-19 Phishing Simulation Result by Age

During COVID-19 phishing simulation for Group 1, three students (60.00%) were aged between 21-30 years old, one student (20.00%) was aged between 31-40 years old, and one student (20.00%) was aged between 41- 50 years old. For Group 2, both students (100.00%) were aged between 21-30 years old and for Group 3, there were two students (50.00%) from both 21-30 years old and 31-40 years old age category.

### 4.2.3 Faculty

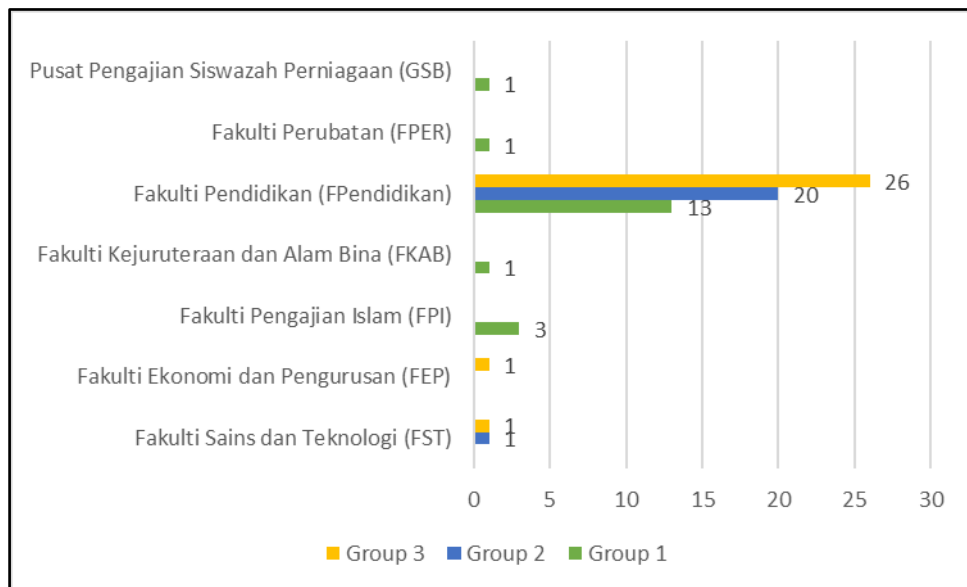


Figure 4.22 Job Scam Phishing Simulation Result by Faculty

The third demographic analysis of the student groups was by faculty. For Group 1's Job Scam phishing simulation, the highest number of students 68.41% (13) that were successfully phished were from *Fakulti Pendidikan (FPendidikan)*. Followed by three students (15.79%) from *Fakulti Pengajian Islam (FPI)*. *Fakulti Kejuruteraan dan Alam Bina (FKAB)*, *Fakulti Perubatan (FPER)*, and *Pusat Pengajian Siswazah Perniagaan (GSB)* each had one student (5.26%) that submitted their data.

*Fakulti Pendidikan (FPendidikan)* had the highest number for Group 2 as well with 20 students (95.24%) and *Fakulti Sains dan Teknologi (FST)* had one student (4.76%). For Group 3, 26 students (92.86%) were from *Fakulti Pendidikan (FPendidikan)*, one student (3.57%) from *Fakulti Sains dan Teknologi (FST)* and one student (3.57%) from *Fakulti Ekonomi dan Pengurusan (FEP)*.

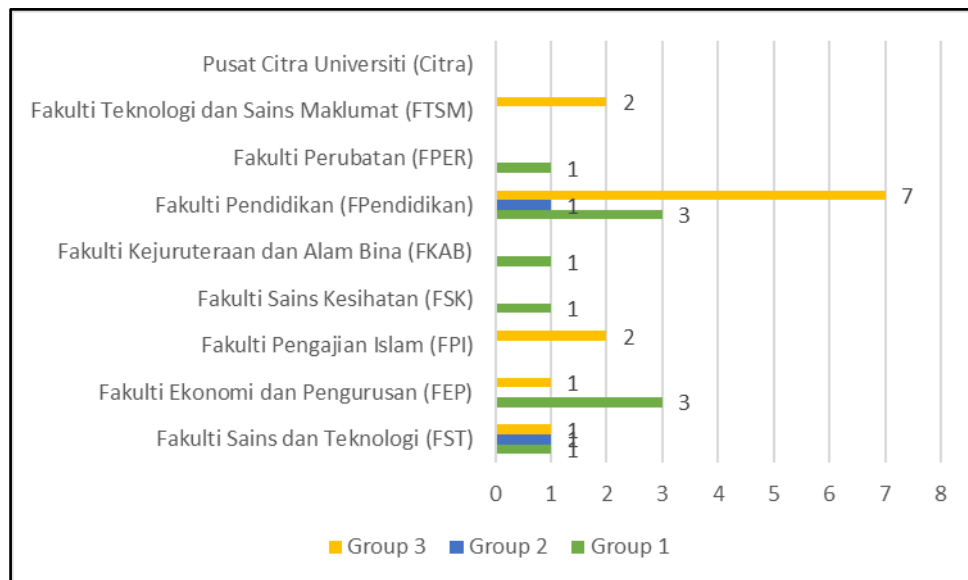


Figure 4.23 Password Reset Phishing Simulation Result by Faculty

During Group 1's Password Reset phishing simulation, both *Fakulti Ekonomi dan Pengurusan (FEP)* and *Fakulti Pendidikan (FPendidikan)* had three students (30.00%) submit their credentials. While *Fakulti Sains dan Teknologi (FST)*, *Fakulti Sains Kesihatan (FSK)*, *Fakulti Kejuruteraan dan Alam Bina (FKAB)*, *Fakulti Perubatan (FPER)* each had one student (10.00%) submit their credentials. For Group 2, both *Fakulti Sains dan Teknologi (FST)* and *Fakulti Pendidikan (FPendidikan)* each had one student (50.00%) shared their data.

Meanwhile, the number of students that submitted their data for Group 3 were seven students (53.85%) from *Fakulti Pendidikan (FPendidikan)*, two students (15.38%) from *Fakulti Teknologi dan Sains Maklumat (FTSM)* and *Fakulti Pengajian*

*Islam (FPI)*, and one student from *Fakulti Sains dan Teknologi (FST)* and *Fakulti Ekonomi dan Pengurusan (FEP)*.

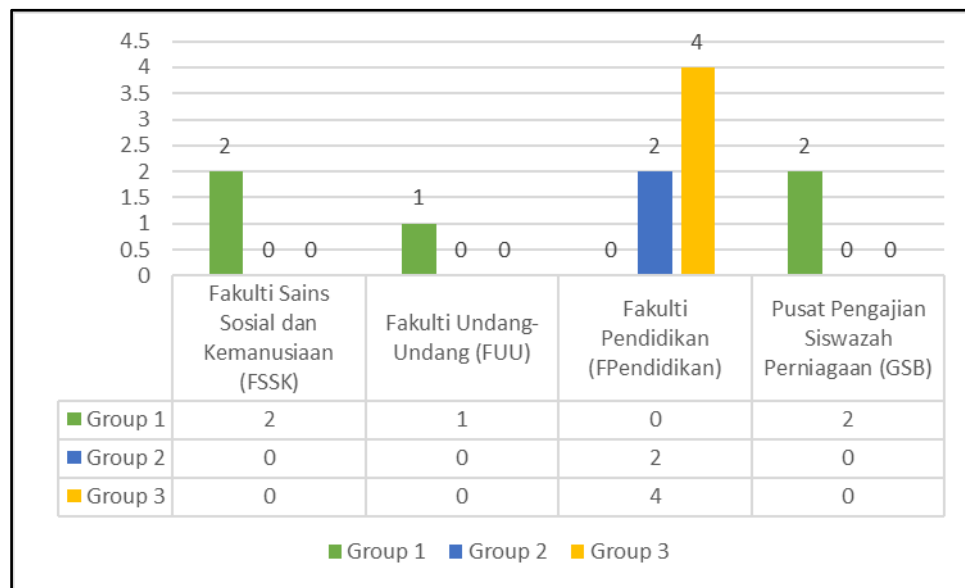


Figure 4.24 COVID-19 Survey Phishing Simulation Result by Faculty

According to Figure 4.24, Group 1 had two students (40.00%) from *Fakulti Sains Sosial dan Kemanusiaan (FSSK)* and *Pusat Pengajian Siswazah Perniagaan (GSB)* and one more student from *Fakulti Undang-Undang (FUU)*. For both Group 2 and Group 3, two students (100.00%) and four students (100.00%) were from *Fakulti Pendidikan (FPendidikan)*.

#### 4.2.4 Education Level

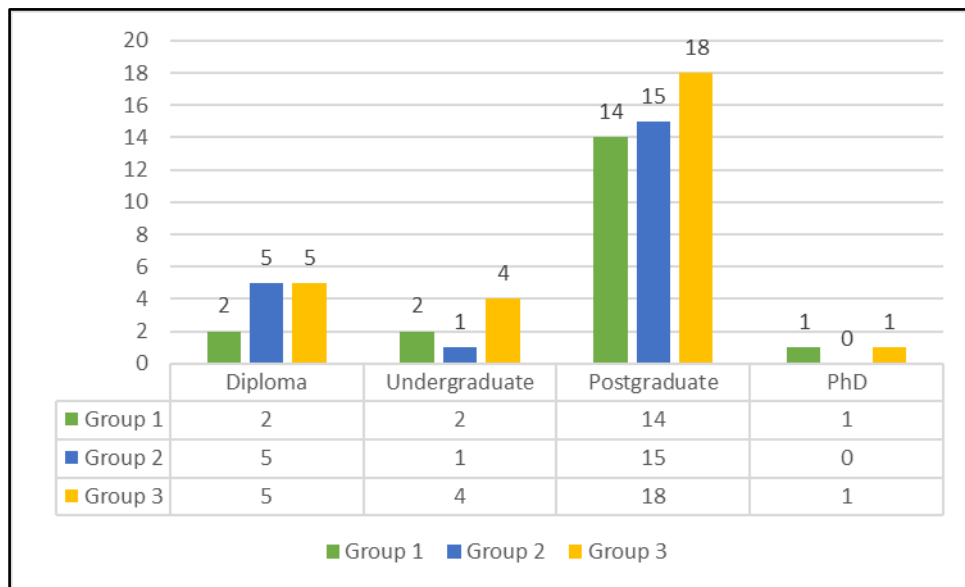


Figure 4.25 Job Scam Phishing Simulation Result by Education Level

The final demographic analysis of the student groups was by their education level. For Group 1, 14 Postgraduate students (73.68%), two Diploma and two Undergraduate students (10.53%), and one (5.26%) PhD student submitted their data. For Group 2, 15 students (71.43%) were from Postgraduate, five students (23.81%) were from Diploma, and one student (4.76%) were from Undergraduate. For Group 3, 18 students (64.29%) were from Postgraduate, five students (17.86%) were from Diploma, four students (14.29%) were from Undergraduate, and one student (3.57%) was from PhD.

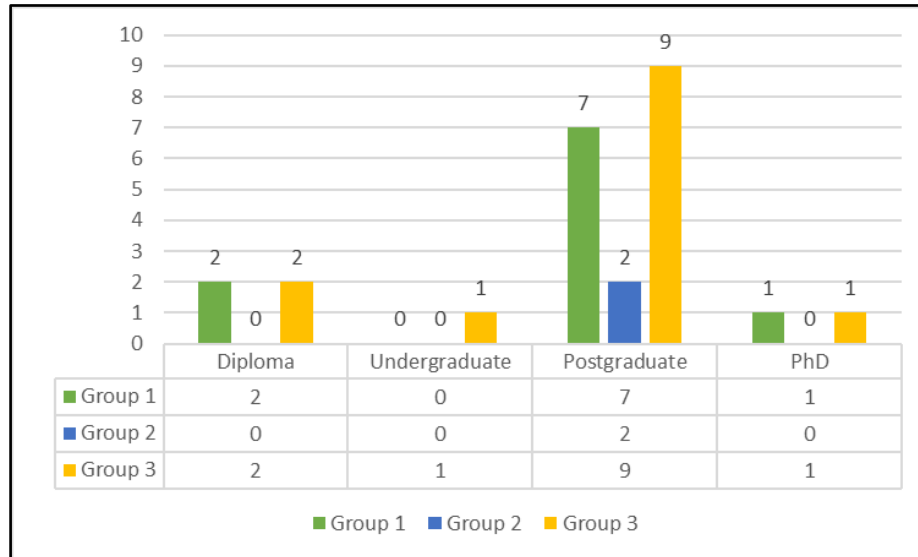


Figure 4.26 Password Reset Phishing Simulation Result by Education Level

For Group 1, seven Postgraduate students (70.00%), two Diploma students (20.00%), and one PhD student (10.00%) submitted their data during Password Reset phishing simulation. For Group 2, both students (100.00%) were from Postgraduate. While for Group 3, nine students (69.23%) were from Postgraduate, two students (15.38%) were from Diploma, and one student (7.69%) each from both Undergraduate and PhD.

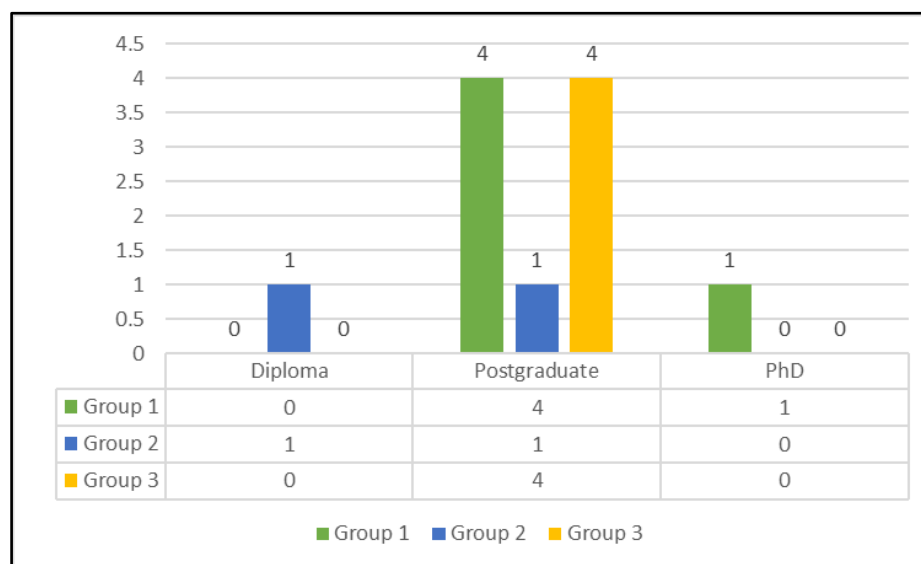


Figure 4.27 COVID-19 Survey Phishing Simulation Result by Education Level