

**CYBERSECURITY RESILIENCE THROUGH
PHISHING SIMULATION: A CASE STUDY OF
FEDERAL POLYTECHNIC BALI, NIGERIA**

HUSSEINI USMAN YARO

UNIVERSITI KEBANGSAAN MALAYSIA

CYBERSECURITY RESILIENCE THROUGH PHISHING SIMULATION:
A CASE STUDY OF FEDERAL POLYTECHNIC BALI, NIGERIA

HUSSEINI USMAN YARO

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

FACULTY SCIENCE AND TECHNOLOGY
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2025

**CYBERSECURITY RESILIENCE THROUGH PHISHING SIMULATION:
A CASE STUDY OF FEDERAL POLYTECHNIC BALI, NIGERIA**

HUSSEINI USMAN YARO

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

**FAKULTI SAINS DAN TEKNOLOGI
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI
2025**

DECLARATION

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

I acknowledge the use of ChatGPT and typeset.io to generate an outline for the dissertation. I entered the following prompt: Provide an outline of Phishing Simulation and awareness. I used the result at the starting point of the project task as a hint and helped the dissertation. The AI-generated output was modified and replaced with my ideas based on the research.

I also acknowledge the use of Grammarly and Quillbot in helping me review my writing at the final stage of preparing my report. I used the following features: Clarity, correctness, and prompt suggestions

05 February 2025

HUSSEINI USMAN YARO
P132148

ACKNOWLEDGEMENT

All gratitude belongs to Allah; I am truly blessed to have completed my project. As I reflect on this achievement, I thank several individuals who played a crucial role in my success. Foremost, I would like to convey my appreciation to my supervisor, Assoc. Prof. Dr. Masnizah Binti Mohd, for her unwavering support throughout the study and generously dedicating her time to instructing me in various techniques. I am thankful for her guidance and the opportunities she has afforded me.

I also want to express my gratitude to Dr. Wandeep Kaur a/p Ratan Singh, the program coordinator, for consistently making time to provide instruction. Additionally, I would like to recognize Dr. Rossilawati Sulaiman, whose contributions have significantly impacted my progress.

I want to express my profound gratitude to my parents, Alhaji Usman Yaro and Laraba Abba Mama, along with my relatives. Your consistent support, encouragement, and genuine interest in my studies have been invaluable. I express my heartfelt gratitude to my brother, Dr. Mohammed Usman, for his unwavering support in my educational journey. His consistent encouragement has been a pillar throughout my life. In moments of frustration, he patiently stood by me, celebrated even the smallest victories, and offered a listening ear whenever I needed it.

To my dearest wife Hafsa and children Ummu'Abiha, Uthaimen, Fawzan, and Nurain, your warmth and grace light up my world, and I dedicate every heartbeat to the beautiful journey together.

I gratefully acknowledge the Tertiary Education Trust Fund (TETFUND) for its generous sponsorship of my Master's degree program. I also appreciate the support and academic guidance provided by the Federal Polytechnic Bali, which greatly facilitated the successful completion of this research.

In conclusion, my gratitude extends to my friends and fellow students for their unwavering support and encouragement. The community I've built at Universiti Kebangsaan Malaysia is vast and diverse, making it impossible to acknowledge everyone by name. The memories we have created together are unforgettable, and I look forward to maintaining our connections in the future.

ABSTRAK

Dengan teknologi yang semakin terintegrasi dalam operasi harian, organisasi menjadi lebih terdedah kepada ancaman siber, khususnya serangan kejuruteraan sosial seperti pancingan data. Kajian ini mengkaji keberkesanan simulasi pancingan data dalam meningkatkan ketahanan keselamatan siber di kalangan kakitangan di Politeknik Persekutuan Bali (FPB), Nigeria. Simulasi ini memanfaatkan insentif kewangan—tawaran bonus selama 13 bulan—yang mengeksploitasi motivasi kewangan dan mencapai kadar respons yang tinggi. Kajian ini menilai kerentanan kakitangan akademik dan bukan akademik, dengan penemuan menunjukkan bahawa kakitangan akademik lebih terdedah, mencatat kadar penglibatan 29.6% berbanding 12.1% untuk kakitangan bukan akademik. Pendorong utama untuk menjadi mangsa termasuk alamat e-mel yang dikenali dan insentif kewangan, dengan kadar respons masing-masing 98% dan 95%, menekankan keperluan untuk latihan dalam mengesahkan kesahihan. Tambahan pula, 43.2% daripada kakitangan yang mengenal pasti percubaan phishing tidak mengambil sebarang tindakan lanjut, sementara seramai 22.5% yang melaporkannya, menunjukkan keperluan untuk meningkatkan mekanisme pelaporan. Insiden pasca simulasi, peserta menunjukkan peningkatan yang signifikan secara statistik dalam kesedaran keselamatan siber, dengan penilaian pengetahuan sendiri meningkat dan 81.1% menyokong simulasi berkala. Selain itu, 83.8% peserta mengakui keberkesanan simulasi dalam meningkatkan kesedaran pancingan data. Kajian ini menekankan nilai latihan keselamatan siber yang berterusan dan interaktif yang diketuai oleh unit ICT, sistem amaran yang dipertingkatkan, dan latihan yang disesuaikan mengenai pengenalan taktik pancingan data. Cadangan ini bertujuan untuk mengukuhkan pertahanan FPB terhadap ancaman kejuruteraan sosial dan membina budaya kewaspadaan keselamatan siber di kalangan kakitangan.

ABSTRACT

With technology increasingly integrated into daily operations, organizations are more vulnerable to cyber threats, particularly social engineering attacks like phishing. This study examines the effectiveness of phishing simulations in enhancing cybersecurity resilience among staff at Federal Polytechnic Bali (FPB), Nigeria. The simulation uses an approach of offering a 13-month bonus to encourage staff to respond. This approach was successful and obtained a high response rate. The study assessed the susceptibility of academic and non-academic staff, with findings showing that academic staff were more vulnerable, recording a 29.6% engagement rate compared to 12.1% for non-academic staff. Key motivators for falling victim included a familiar email address and financial incentives, with response rates of 98% and 95%, respectively, emphasizing the need for training on verifying authenticity. Additionally, 43.2% of staff who identified the phishing attempt took no further action, while only 22.5% reported it, highlighting a need for improved reporting mechanisms. Post-simulation, participants showed a statistically significant increase in cybersecurity awareness, with self-assessed knowledge ratings improving and 81.1% supporting regular simulations. Moreover, 83.8% of participants acknowledged the simulations' effectiveness in enhancing phishing awareness. The study underscores the value of continuous, interactive cybersecurity training led by the ICT unit, improved alert systems, and tailored training on recognizing phishing tactics. These recommendations aim to strengthen FPB's defenses against social engineering threats and cultivate a culture of cybersecurity vigilance among staff.

2.6.3	Italian Hospital	19
2.6.4	King Abdulaziz University (KAU), Saudi Arabia	19
2.6.5	Current Phishing Trends	24
2.7	Human Factors and Susceptibility	25
2.7.1	Educational Institutions as a Unique Cybersecurity Target	26
2.7.2	User Awareness	27
2.7.3	Countermeasures and Solutions	29
2.8	Summary	29
 CHAPTER III METHODOLOGY		
3.1	Overview	31
3.2	Research Design	31
3.2.1	Implemented Methodology	31
3.3	Simulation	35
3.3.1	Preparation Stage	36
3.3.2	Planning Stage	36
3.3.3	Design Stage	36
3.3.4	Execution Stage	39
3.3.5	Analysis Stage	41
3.4	POPULATION and SAMPLING TECHNIQUES	41
3.4.1	Population	41
3.4.2	Target Group	41
3.4.3	Sampling Techniques	42
3.5	data COLLECTION METHODS	42
3.5.1	Survey	42
3.5.2	Phishing Simulation	42
3.5.3	Remote Questionnaire	42
3.6	Tools and Instruments For Data Analysis	43
3.7	Ethical Considerations	43
3.8	Limitations	43
3.9	Summary	44
 CHAPTER IV RESULTS AND DISCUSSION		
4.1	Introduction	45
4.2	Pre-Simulation Survey Analysis	45
4.2.1	Demographic Analysis	45
4.2.2	Cybersecurity Practices Analysis	47

	4.2.3	Level of Awareness About Phishing Before the Study	49
4.3		Phishing Simulation Analysis	50
4.4		Post-Simulation Survey Data Analysis	52
4.5		Change In Participant's Self-Assessment Rating Before and After Study	64
4.6		Summary	66
CHAPTER V	CONCLUSION AND FUTURE WORKS		
5.1		Introduction	67
5.2		Discussion and Findings	67
	5.2.1	Objective 1: To measure the current state of cybersecurity resilience at the Federal Polytechnic Bali, Nigeria, particularly to phishing attacks	70
	5.2.2	Objective 2: To design and implement phishing simulation exercises tailored to the institution's specific context and threat landscape	70
	5.2.3	Objective 3: To evaluate the effectiveness of phishing simulation in improving staff awareness, preparation and response to phishing threats	70
5.3		Contribution	71
5.4		Limitations and Future Work	72
REFERENCES			73
APPENDICES			
Appendix A		Questionnaire	79

LIST OF TABLES

Table No.		Page
Table 2.1	Related Caes Studies Summary	24
Table 3.1	Phases and mapped objectives of phishing simulation	34
Table 3.2	Indicators of Phishing Red Flags	37
Table 3.3	Implementation Timeline	40
Table 4.1	Cybersecurity Practices	47
Table 4.2	Self-Assessment Rating Scale Before Simulation	49
Table 4.3	Post-simulation Survey Q1	53
Table 4.4	Response to the '13-Month Bonus	54
Table 4.5	Action After Receiving the Email	54
Table 4.6	Phishing Email Recognition as Suspicious	55
Table 4.7	Factors Identifying Emails as Suspicious	56
Table 4.8	Factors Influencing Email Trust	57
Table 4.9	Pre-Study Phishing Encounter	58
Table 4.10	Phishing Simulation Awareness	59
Table 4.11	Phishing Awareness Before Study Participation	60
Table 4.12	Phishing Awareness Simulation Impact	61
Table 4.13	Self-Assessment Rating Scale	62
Table 4.14	Need for Regular Phishing Simulations	63
Table 4.15	Expected scale assessment value before and after the study	64
Table 4.16	Chi-Square Test Contributions	64

LIST OF FIGURES

Figure No.		Page
Figure 2.1	Taxonomy of Social Engineering (Source: Salahdine, et al. 2019)	9
Figure 2.2	Components of Social Engineering (Source: Salahdine, et al. 2019)	10
Figure 2.3	Forms of Social Engineering (Source: Salahdine, et al. 2019)	12
Figure 2.4	Phishing Process (Source: Jain, et al 2022)	15
Figure 2.5	Phishing Attacks Statistic (Source: Phishing Activity Trends Report Quarter 2023)	16
Figure 3.1	Research Design	33
Figure 3.2	Phishing Email Sent	38
Figure 3.3	Fake Google Form for Data Capture	39
Figure 4.1	Pre-simulation Survey Response	46
Figure 4.2	Gender and Age Group Distribution	46
Figure 4.3	School and Staff Category Chart	47
Figure 4.4	Familiarity with Cybersecurity	49
Figure 4.5	Self-Assessment Rating Scale Before Simulation Chart	50
Figure 4.6	Phishing Simulation Response Summary	51
Figure 4.7	Phishing Simulation Response Rate by School	51
Figure 4.8	Response Rate by Departments	52
Figure 4.9	Post-simulation Survey Q1 Pie Chart	53
Figure 4.10	Respond to the '13-Month Bonus Payment	54
Figure 4.11	Action After Receiving the Email	55
Figure 4.12	Phishing Email Recognition as Suspicious	56
Figure 4.13	Factors Identifying Emails as Suspicious	56
Figure 4.14	Factors Influencing Email Trust	58
Figure 4.15	Pre-Study Phishing Encounter	59
Figure 4.16	Phishing Simulation Awareness	59
Figure 4.17	Phishing Awareness Before Study Participation	60
Figure 4.18	Phishing Awareness Simulation Impact	61

Figure 4.19	Self-Assessment Rating Scale Chart	62
Figure 4.20	Perception of the Need for Regular Phishing Simulations Chart	63

LIBRARY FTSM

LIST OF ABBREVIATIONS

ABEET	Agric and Bio-Environmental Engineering Technology
ACC	Accountancy
AGT	Agricultural Technology
AHP	Animal Health Production
APWG	Anti-Phishing Working Group
BAM	Business and Administration Management
BT	Building Technology
CE	Computer Engineering
CS	Computer Science
ETRP	Entrepreneur
FPB	Federal Polytechnic Bali
GF	Google Form
GST	General Study
LIB	Library
PAD	Public Administration Department
SAT	School Agricultural Technology
SBMT	School of Business and Administration Management Technology
SET	School of Engineering Technology
SLT	Science Laboratory Technology
SST	School of Science and Technology
STAT	Statistics
UKM	Universiti Kebangsaan Malaysia

CHAPTER I

INTRODUCTION

1.1 RESEARCH BACKGROUND

The use of information and communications technologies has led to novel progressions in our daily lives and precipitated an acceleration in the use and production of electronic devices. As the world has moved into the cyber generation, an increasing number of scepticisms related to the use of the digital environment have transpired, presenting new digital security risks and challenges. Over the last decade, a remarkable growth in the number of cybercrimes has been documented worldwide. These crimes have been successfully carried out through the Internet; including deception, identity stealing, tricks, cyberstalking, and cyber terrorism (Aljeaid et al. 2020). An increasing number of internet resources and research highlight the effectiveness of email phishing techniques. 96% of social attacks arrive via email, and 85% of IT breaches include human involvement. Phishing is a prevalent and remarkably effective tactic (Tomidić, 2023).

Ahmed (2021) noted that social engineering (SE) describes events where an information system is compromised by the application of social techniques. Phishing is one of the techniques used to compromise sensitive data. According to Chanti et al. (2022), phishing is a deceitful action through which the phisher influences users into revealing their sensitive data to gain monetary. Phishing attempts often target emails since people check their accounts both at home and at work. Adversaries can choose from a variety of tactics when emails are used as a vector for phishing attacks, including posing as the sender, adding a malicious payload, or including malicious links within the content of the email's body (Casagrande et al. 2023). Phishing simulations are a necessary tool for employee training, on how to identify and counter phishing attacks

that target organizations. Phishing simulation, as mentioned by Rizzoni et al. (2022), tests employees' capacity to recognize phishing emails through a controlled and approved fake attack. The importance of these simulations in preventing cybercrimes has been shown by multiple research papers and their broad availability from different cyber awareness training providers.

It is well established from a study by Casagrande et al. (2023) that academic institutions face significant threats from phishing attacks, which can result in substantial financial losses and compromised academic property. The study by Casagrande et al. highlights the severity of this issue. For example, the threat actor known as the Silent Librarian deployed deliberate spear phishing assaults on academic establishments in Iran. They also gained illegal access to computer networks, stole confidential information, and sold it to Iranian clients that included Iranian colleges and the government. University email templates, addresses, websites, and branding were impersonated in order to drive victims to fraudulent university library login pages. Silent Librarian stole around 3.4 billion dollars in intellectual property between 2013 and 2017 and compromised 8,000 university accounts. Moreover, Lancaster University in England experienced a sophisticated phishing attack that led to a data breach, and an analysis of email security revealed thousands of compromised accounts at top universities (Casagrande et al. 2023). These incidents underscore the urgent need for academic institutions to prioritize cybersecurity and protect against phishing attacks.

Like many other academic institutions, Federal Polytechnic Bali, Nigeria faces the risk of phishing attacks. However, there is a need for more research on the effectiveness of phishing simulation in the context of educational institutions, particularly in Nigeria. Federal Polytechnic Bali, Nigeria, is an intriguing case study given of its unique challenges and weaknesses. Because it is an academic institution, its user are broad and comprises teachers, staff, and students with varying degrees of cybersecurity expertise and awareness.

1.2 PROBLEM STATEMENT

Phishing attacks have become visible as a critical cybersecurity threat, by making the use of both technological vulnerabilities and human psychology to deceive users into disclosing sensitive information. These attacks are increasingly employing different forms of techniques such as email, website, and social media phishing to pretend to be a trusted body or organization (Borate et al. 2024). AntiPhishing Working Group describes phishing as a crime using both social engineering and technical deception to rob sensitive data. According to Marco et al. (2022) cyber threats in educational institutions have gradually become the sole target for phishing attacks, presenting a risk to the security of sensitive information. The effectiveness of present cybersecurity measures in the context of phishing remains uncertain, despite the efforts to raise awareness. Marco et al. (2022) stated that the absence of regular phishing simulation exercises limits the ability of staff and students to identify and respond to phishing threats effectively, resulting in significant monetary losses, reputational harm, and compromise of intellectual property.

The Federal Polytechnic Bali lacks strategies to mitigate vulnerabilities, and the absence of these strategies may leave the Federal Polytechnic Bali with more risks and cyber-attack threats. Many users have been deceived into clicking on fake website links found in the email. Usually, visible phishing emails are sent in large numbers and have phishing characteristics. According to ICT coordinator, Mohammed Hamidu state that the lack of awareness regarding phishing tactics makes the staff more susceptible to phishing attacks. He continues saying that as the FPB continues to integrate technology into its operations, the risk of phishing attacks increases, especially through platforms like email and WhatsApp, which are commonly used for communication. Implementing robust phishing simulation exercises and awareness of the existing approach reduces cyber breaches (Anawara et al. 2019). These initiatives should not only aim at cyber attention but also empower employees with the ability and skills to detect, foil, and report phishing attempts effectively.

1.3 RESEARCH QUESTIONS

This research aims to answer two main questions.

1. What is the current level of cybersecurity awareness among employees at Federal Polytechnic Bali, Nigeria?
2. Can phishing simulation exercises improve cybersecurity resilience at Federal Polytechnic Bali, Nigeria?

1.4 RESEARCH OBJECTIVES

By adopting an existing phishing simulation by Norhafizah (2017), an endeavor to address the lack of phishing attack awareness at Federal Polytechnic Bali. The following objectives are:

1. to measure the current state of cybersecurity resilience at the Federal Polytechnic Bali, Nigeria, particularly to phishing attacks.
2. to design and implement phishing simulation exercises tailored to the institution's specific context and threat landscape.
3. to evaluate the effectiveness of phishing simulation in improving staff and student awareness, preparedness, and response to phishing threats.

The research questions and objectives in this study are closely aligned to ensure a coherent and logical flow. The first research question (RQ1), which seeks to understand the current level of cybersecurity awareness among employees at Federal Polytechnic Bali, Nigeria, is addressed by two objectives. Research Objective 1 (RO1) focuses on measuring the current state of cybersecurity awareness and resilience to phishing attacks. At the same time, Research Objective 3 (RO3) evaluates the effectiveness of phishing simulation exercises in improving staff and student awareness, preparedness, and response to phishing threats. The second research question (RQ2), which examines whether phishing simulation exercises can improve cybersecurity resilience, is supported by Research Objective 2 (RO2) and Research Objective 3 (RO3). RO2 involves designing and implementing phishing simulation exercises

tailored to the institution's specific context and threat landscape, while RO3 assesses the outcomes of these simulations. Together, these objectives ensure that the study comprehensively addresses both research questions, providing actionable insights into cybersecurity resilience and awareness.

1.5 RESEARCH SCOPE

This study explores the existing work on the effects of phishing simulation, which builds and extends on previous work in this area, and also dissects the effects of phishing simulation on the institution's cybersecurity strength. This study reviews the present cybersecurity stance at the Federal Polytechnic Bali, drafting and deploying a phishing simulation method, and its effectiveness in transforming employees' cybersecurity awareness. The research will also include a sample of employees participating in the study.

Research questions, objectives, and methodology are designed to cater for a comprehensive understanding of the effectiveness of phishing simulation in enhancing cybersecurity resilience and its potential for integration into the institution's existing cybersecurity framework. However, the study is limited to Federal Polytechnic Bali, Nigeria, its results will facilitate the development of conceptual cybersecurity solutions and foster a more secure cyber environment for educational institutions.

1.6 SIGNIFICANCE OF STUDY

This study adopts the standard simulation method of specific phishing approaches designed by Norhafizah (2017), which helps employees in cybersecurity awareness and behaviour, providing insights and effectiveness in promoting a culture of cybersecurity. There is a need for more cybersecurity research at Federal Polytechnic Bali, Nigeria. This study contributes to filling this knowledge gap. The phishing simulations approach is important and provides a practical approach to enhancing cybersecurity resilience, making it a valuable resource for organizations to reduce the risk of successful phishing attacks.

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

1.7 THESIS OUTLINE

This project will comprise five chapters. The first chapter of this work includes an introduction that provides an outline of the research background, and the research objectives to be achieved. The research questions, research problem statement, and the scope that will be conducted. The second chapter deals with a review of related phishing simulations, including case studies of phishing attacks, and discusses some data breaches in educational institutions. The previous literature review is used to help better understand the study. The third explains the methodological approaches that will be carried out throughout this research. It explains details about research methods, data collection methods, and sample selection. The fourth presents and intensively interprets the findings of the data collected, which relate to the based on defined objectives. The last reflects on the summary, conclusion, and discussion of the study, and point out suggestions for future research.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

Phishing simulation has emerged as a critical tool for enhancing cybersecurity resilience. Organizations can assess and improve their defensive mechanisms by simulating phishing attacks, educating their workforce, and reducing susceptibility to real threats. According to Jain et al. (2021), phishing is a prevalent cybercrime that involves deceptive attempts to obtain sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in electronic communications. It poses significant risks to individuals and organizations, leading to financial losses and identity theft (Kheruddin et al. 2024). This literature review explores various aspects of phishing simulation, including its methodologies, impacts on awareness and behaviour, best practices for implementation, and countermeasures.

2.2 INFORMATION SECURITY

A review paper by Yee et al. (2021) outlines that Information Security aims to safeguard data in three ways: confidentiality, integrity, and availability. The organization must effectively manage risks associated with information security, including unauthorized modifications, unlawful access, and disruptions. Every sector has its responsibility to enhance the knowledge in the field of information security to secure the network environment. Each organization is committed to advancing knowledge in information security to safeguard network environments. Establishing a secure network that maintains user information in a confidential status ensures user authentication and messages should not be altered during transmission while also preventing common internet attacks. Organizations should take responsibility for securing their information and data so hackers will not attack them. Employee data should be addressed to ensure

data security. Information should be safeguarded to prevent data from being leaked to unauthorized people. Information security in the digital age can be correctly disclosed when its confidentiality becomes compromised, wrongly altered when its integrity is put at risk, and destroyed if its availability is endangered.

According to Chee et al. (2020), Cybersecurity has potential dangers connected with the likelihood of cyber threats that target assets in an organisation. In the current era, internet connectivity has become very easy for users to access; therefore, information systems have become more vulnerable to human fallibility, and technological failures (Boltz 1999; Talet et al. 2014). Fadzline (2020) shows that society must protect itself from the harm of cyber threats via proactive steps and measures to detect the early signs of cyber threats. Lately, in recent times, the use of numerous digital devices and the ability to use online services have progressively expanded the information security obstacles. Therefore, safeguarding the information becomes a significant task to make attention, especially in the private and public sectors (Mouton et al. 2014).

2.3 SOCIAL ENGINEERING

According to Grassegger et al. (2021), social engineering is a form of attack that tries to manipulate employees into revealing confidential information or performing actions that threaten organizations' digital security. Wang, et al. (2020) describe social engineering from the security standpoint is an assortment of continuous activities that involves new types and tactics increasingly all the time, especially, since it has advanced and developed obviously in the last 20 years. It is like an advancing target. In every part of history social engineering will continue to exist in different types.

Acquiring sensitive data, such as passwords, and credit card information, and getting to the system without official authorisation poses the trust and the links with others who have access to such data. Attackers via social engineering mostly target individuals with 97%, meanwhile, only 3% of malware attempts to succeed in technological failures (Frumento, E. 2018). Krombholz, et. al. (2014) show that social engineers are a group of hackers whose concern is convincing and encouraging individuals of specific rank to execute harmful activities such as disclosing sensitive

data. This is contrary to that of Breda et al. (2017) who show the attention of hackers on cybersecurity is primarily to inspire victims to expose sensitive data, or to carry out act that breach security set of rules. 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 addicted.

Conteh et al. (2021) highlight strategies social engineering attackers may use to acquire visibility or sensitive information. These strategies range from phishing to dumpster diving, a combination of human and technical tactics may be used to gather information about an individual or acquire access to an organization for proactive and effective phishing attacks. Their study outlines four steps for the social engineering attack process, which involves information gathering, relationship building, implementation, and exploitation.

2.4 TAXONOMY OF SOCIAL ENGINEERING ATTACKS

Depending on the nature of the attacks, social engineering can be identified into two categories human-based or computer-based as graphically displayed in Figure 2.1, (Salahdine, et al. 2019).

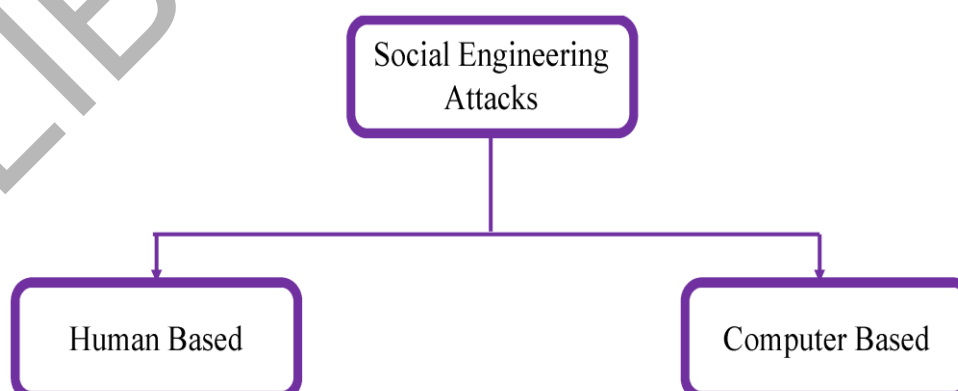


Figure 2.1: Taxonomy of Social Engineering

Source: Salahdine, et al. 2019

Salahdine, et al. (2019) highlight that human-based attacks convince a small number of victims, and the hackers collect the intent information by cooperating in communication with the target during the acts. Similarly, in software-based they convince several victims in a fraction of a second, the attackers employ digital devices including computers or smartphones to collect data from them.

2.4.1 Components of Social Engineering

In line with how the attack is carried out, the social engineering attacks can be grouped into three classes, social, technical, and physical-based attacks (Salahdine, et al. 2019) as depicted in Figure 2.2.

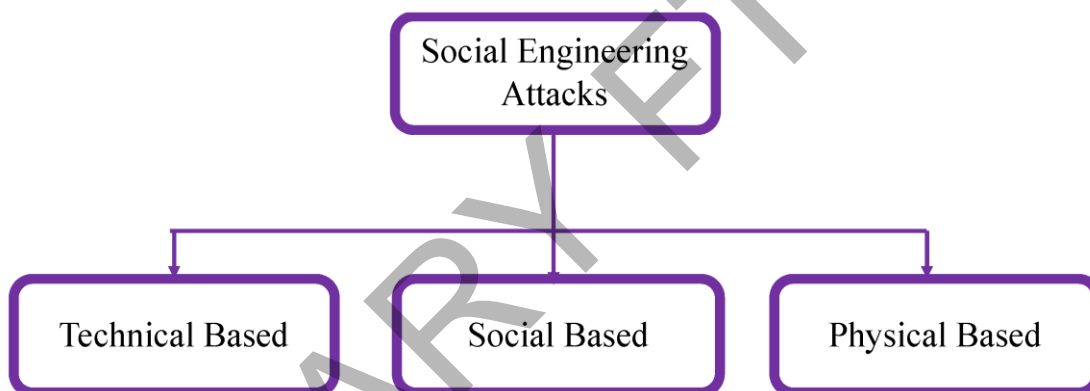


Figure 2.2: Components of Social Engineering

Source: Salahdine, et al. 2019

Pokrovskaja (2017) points out that physical-based pertains to physical activity to gather information regarding the victim, for instance, such assaults include scouring in the trash for precious documents. Patil, et al (2016) highlight that social-based attacks comprise human interaction, and the attack is most harmful due to human involvement. In social-based attacks, the attacker associates with the victim and plays on their dynamic behaviour—for instance, baiting and spear phishing. Using social media platforms and websites, cybercriminals employ Technical-based attacks to get sensitive information, including passwords, credit card numbers, and security questions (Kalniņš, et al. 2017).

This study is closely related to the notions of social-based and technical-based attacks. Social-based attacks, highlighted by Patil et al. (2016), involve human interaction where the attacker exploits the victim's behaviour, such as in baiting and spear phishing. These types of attacks are directly relevant to phishing simulations because they input the use of tactics to influence individuals to achieve a specific goal, making them crucial for training individuals to recognize and respond to such threats. Technical-based attacks, as described by Kalniņš et al. (2017), use digital methods like social media and websites to obtain sensitive information. These attacks are also highly pertinent to phishing simulations since they often involve deceptive emails and fake websites, which are common tactics in phishing. By incorporating these types of attacks into the simulations, the study can provide realistic training scenarios that enhance participants' ability to detect and avoid phishing attempts, thereby strengthening cybersecurity resilience. While physical-based attacks, discussed by Pokrovskaja (2017), involve gathering information through physical means like searching through trash, they are less directly related to phishing simulations. However, including awareness of such physical security measures can contribute to a more comprehensive cybersecurity training program, complementing the digital focus of the simulations.

2.4.2 Forms of Social Engineering

By drawing the abovementioned components of social engineering, Salahdine, et al. (2019) have been able to show examples of different forms of social engineering assault which comprises phishing, impersonation on help desk calls, shoulder surfing, dumpster diving, stealing valuable documents, diversion theft, fake software, baiting, quid pro quo, pretexting, tailgating, Pop-Up windows, Robocalls, ransomware, online social engineering, reverse social engineering, and phone social engineering. These examples are graphically displayed in Figure 2.3.

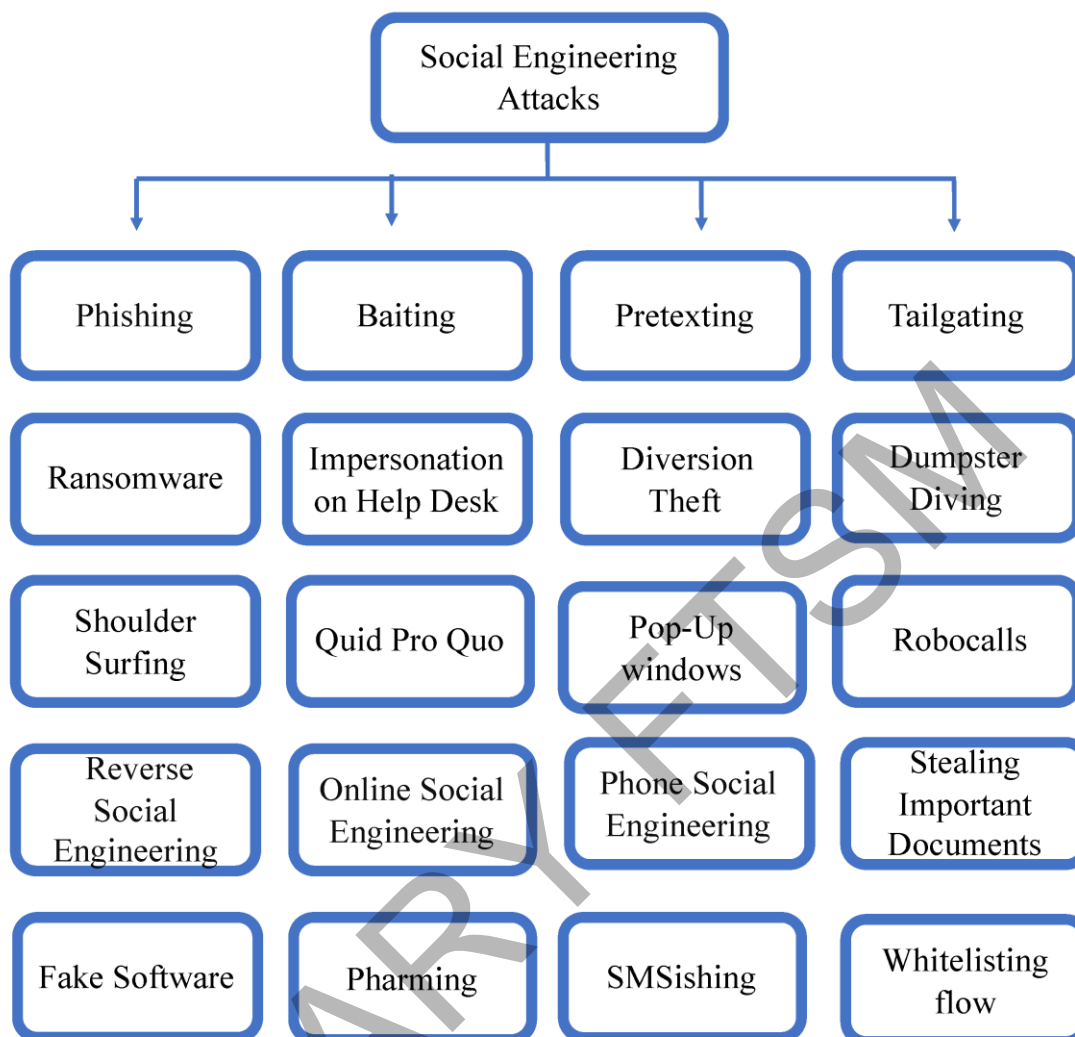


Figure 2.3: Forms of Social Engineering

Source: Salahdine, et al. 2019

Figure 2.3 highlights various social engineering attacks that manipulate individuals into compromising security, many of which relate directly to this study. Phishing, the core of this research, is a widely used technique that employs email or SMS to entice individuals into revealing sensitive information. This techniques of Baiting and Pretexting could be simulated in the phishing exercises of this study by creating scenarios that exploit curiosity or trust, thereby assess employees' ability to identify deceptive messages. Additionally, Pop-Up Windows, Fake Software, and Pharming target users digitally and can be simulated to test whether individual recognize unverified downloads or malicious pop-ups, essential skills for safeguarding against online scams.

Furthermore, the figure highlights Physical and voice-based attacks, such as Tailgating, Impersonation on the Help Desk, Phone Social Engineering, and other components, show that social engineering is not limited to emails; attackers exploit human behaviour in various ways. Therefore, educating staff further reinforces the importance of securing physical documents, understanding early signs of cyber threats, and equipping employees with skills to recognize and respond to both digital and non-digital social engineering tactics.

The components of social engineering outlined by Salahdine et al. (2019) aimed at exploiting human behaviour to gain unauthorized access to information or systems. For this study, the most relevant components are phishing, baiting, pretexting, and online social engineering. Phishing is directly relevant as it involves deceptive emails to extract sensitive information, aligning perfectly with the study's focus on phishing simulations. Baiting, which involves enticing victims with appealing offers leading to malware or data theft, is crucial for teaching participants to recognize and avoid such traps. Pretexting, where attackers fabricate scenarios to obtain information, helps individuals identify and handle suspicious requests for information. Online social engineering, which uses online platforms for deception, is essential for training participants to recognize fraudulent profiles and websites.

2.5 PHISHING PROCESS AND VECTOR

According to Gupta, et al. (2018), phishing is an act of pilfering sensitive data such as financial details and personal information from individuals over the Internet. Phishing attacks may result in the pilfering of sensitive information particularly personal data which involves login identification and passwords to separate online platforms. As a result of exposing confidential data, the user walks into a trap and supplies the information via malicious links or deceptive emails. These lead to data breaches and many severe damaging consequences (Almomani et al. 2013). Phishing poses a great threat to employees of organizations because of the fundamental weakness of the employees in recognizing the threat from phishing hints, as well as the talents of the phisher in perfecting content that considers the perspectives of individuals' emails (Nicholas, et al. 2018). According to Gascon, et al. (2018), phishing attacks form not

only successful hacking techniques to gain access to companies and organizations. However, in the context of recognition and action to reduce the attacks, phishing attacks also pose a real difficulty (Thomas, 2018).

Spear-phishing emails are selectively targeted by nature. Attackers will take advantage of current popular themes and events to mislead their victims into clicking on harmful links. Spear-phishing emails remain an enormous threat and with organizations primarily depending on emails for communication, it has become more crucial to identify the factors that make them successful. One of the most essential components is the human link. With people being the most vulnerable link, it is obvious that the attacker will exploit such vulnerability and attempt to utilize it for their gain. A significant amount of work has been made into safeguarding data from direct cyberattacks, despite this, the most successful breaches have penetrated organizations through mistakes made by humans. Therefore, deeper knowledge of what makes a person fall for spear-phishing emails is crucial in strengthening the human firewall (Alhaddad et al. 2023)

A study by Alhaddad et al. (2023) highlights that spear-phishing email was the most frequent attack technique. The study also shows the Symantec Internet Security Threat Report 2019, indicates that 65% of known groups utilize spear-phishing as a major attack vector. Reports also revealed that 95% of the groups' objectives for such an attack were data gathering. Likewise, the Anti-Phishing Working Group has revealed 46,036 phishing websites, and 44,497 distinct phishing attacks were executed in June 2020. An American security company 'ProofPoint' reported that 88% of businesses had encountered spear-phishing attacks in 2019, and 55% of firms had fallen victim to a successful attack at least once in 2019. Simultaneously, Verizon reported that 22% of breaches phishing was included. Considering these worrisome figures and click rate, analyze how effectively an organization plans for a phishing attack and the elements involved.

2.5.1 Phishing Process

As technology continues to evolve, cybercriminals employ several strategies to gather sensitive information from users. According to Jain et al. (2022), the phishing process

has six stages explicitly: as displayed in Figure 2.4, the first stage is the Planning and Setup stage, which is the stage of discovering and focusing on the target sector to gain secret data. Second is phishing site construction, which is the stage of designing phishing sites that resemble the genuine website of the organisation using distinct online tools to replicate the legitimate website. Third is phishing spreading is the stage where the phisher transmits the link of the phishing website. Fourth, the Installation stage diverts the user to a fake link of the malicious site, because of clicking, the user may arrive by giving confidential data. Fifth, is the Data collection stage, where the phisher retrieves the information supplied by the user over the internet. Lastly, Break-Out stage, in the final stage the attacker removes all the phishing websites and email accounts after obtaining the users' confidential information.



Figure 2.4: Phishing Process

Source: Jain, et al 2022

2.5.2 Phishing Attacks Vectors

Emails are a major vector for phishing efforts since people log their email accounts both at the workplace and in their spare time. When employing emails as vectors for phishing assaults, counterparts can select between numerous techniques, such as impersonating the receivers' email account, embedding a malicious payload, or inserting a malicious link in the email text contents (Casagrande et al 2023). According to Verizon's data breach investigation report (2018), regarding malware-related phishing, the main vectors used by phishing scams are emails, in 96% of social incidents, emails are the most used approximately 92% of attempts breaches while websites account for around 6%.

Phishing is a part of cybercrime that uses social engineering to spread messages through digital communication mediums, including social media platforms sites, SMS, and email. Studies indicate that 65% of phishing attacks are from email and due to the click on hyperlinks affixed with the email received. The Phisher carefully designed a

website and email like the sector's authentic sites and emails to attract an individual's attention to disclose sensitive information. There are several sorts of phishing assaults, the most prevalent of which is spear phishing targeting higher education institutions using students' official emails (Okokpujie, et al. 2023).

2.6 RELATED WORKS

According to the Anti-Phishing Working Group (APWG) 2020 report, the number of phishing websites discovered rose between Q4 2019 and Q1 2020. Moreover, there were around 214,345 distinct phishing sites, and recent phishing assaults have increased since early 2020 and in the year 2021, 83% of institutions reported phishing assaults

In a recent report, APWG's Q4 2023 Phishing Activity Trends Report discloses that the APWG study carefully examines precariously close to five million phishing attacks in 2023, making it a breaking-record year for phishing. APWG Senior Research Fellow highlights that phishing attacks dropped in the mid-year of 2023 because of the termination of operation of the free assessable domain name program called Freenom. However, despite a decline in the first quarter, phishing increased in the latter half of the year. In the final phase of 2024, the APWG noticed 1,007,501 phishing attacks. Figure 2.5 shows the statistics of phishing from 2021-2023.

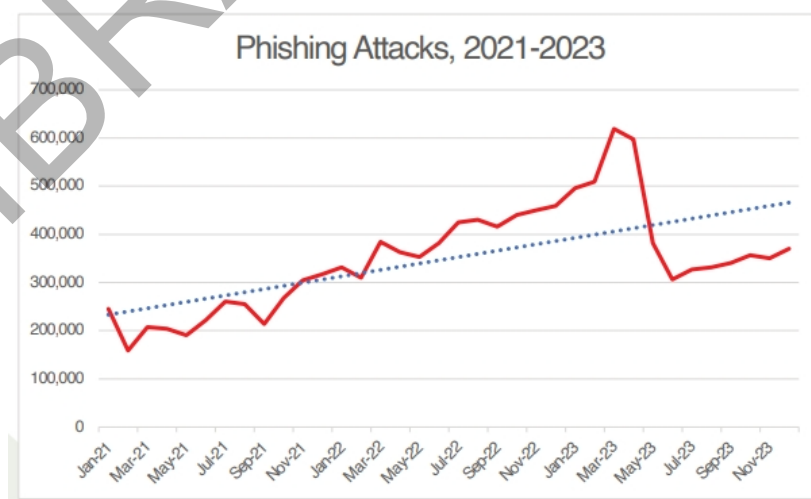


Figure 2.5: Phishing attacks statistic

Source: Phishing Activity Trends Report Quarter 2023

Much of the literature on phishing simulation has emphasized the importance of training on identifying and reporting phishing emails as a component of an organization's information security awareness training program. Training and educating all users on cybersecurity awareness and related responsibilities is essential to cybersecurity risk management. Also, training should be provided to new users and repeated periodically. Organizations are encouraged to enhance the training by conducting exercises that simulate actual cyberattacks. Today, several open-source and commercial tools are readily available to send emails to simulate a phishing attack. Many organizations authorize the using these tools to enhance cybersecurity training and launch phishing emails to generate a simple metric of the percentage of users that were fooled by the phishing email. An organization and its users must be trained before you can test their abilities to detect and respond to phishing. The phishing exercise is not the training itself but a measure of the effectiveness of the provided training. It is also intended to reinforce concepts in the training material. The components of a security awareness training program can vary based on tailoring for the organization (Miranda, 2018).

According to Beu et al. (2023), organizations evaluate employee susceptibility to phishing attacks by conducting regular blinded phishing simulation exercises. These phishing simulations involve sending emails to employees with identifiable phishing cues, such as suspicious sender URLs or spelling errors. Key metrics derived from these simulations are click rate and reporting rate. Click rate displays the percentage of successful phishing attempts by the employees to click the link in an illegitimate email. On the other hand, the reporting rate reflects the percentage of simulated phishing links that were reported using the organization's reporting process for suspected phishing emails, demonstrating proactive awareness of potential threats. In research by Yeng et al. (2022) involving 167 healthcare staff for phishing simulations, 102 (61.1%) engaged with the simulated malicious link, while sixty-five (65) (38.9%) remained impervious to the attack. Additionally, twenty-five (25) participants (24.5%) out of the 102 who visited the link completed the questionnaire included in the research. Thus, seventy seven (77) people (75.5%) did not respond to the survey. The clicking behavior was increased at the beginning of the simulated attack but significantly reduced after the initial two days. Among the 167 staff members who received the simulated phishing email, 61.1% fell victim. Nevertheless, just 25 (24.5%) of the victims completed a

questionnaire, citing various reasons for their vulnerability. For example, seven (7) (68%) of the 25 participants trusted the phishing message's subject, whereas six (6) (24%) were inquisitive.

2.6.1 Universiti Kebangsaan Malaysia (UKM)

Norhafizah et al. (2018) carried out an experimental phishing simulation exercise at the Universiti Kebangsaan Malaysia (UKM) with 553 employees from different faculties, enticement spear-phishing email with the subject matter "Financial Aid" was sent to them. At the end of the simulation, a post-analysis survey was sent. By the end of the survey period, data had been recorded from employees of different faculties, 45% of whom were from the faculty of science and technology while 49% were not from the faculty of science and technology, and the remaining 5% were from other divisions. This indicates that the employees from these faculties had forwarded the content of the email to other units.

Furthermore, 60 responses were collected in the post-analysis survey, the majority of participants (53%) indicated that they had supplied their sensitive data, while the remaining percent identified that the email was apprehensive. Most of the participants believe that the email was genuine from the official due to the identity of the sender and the subject matter of the enticement phishing email. On the contrary, some refused to click the link because the email and website looked questionable.

2.6.2 Japan Advanced Institute of Science and Technology

As reviewed by Norhafizah et. al (2017) Japan Advanced Institute of Science and Technology carried out experimental training for its staff through its security team to improve security awareness of phishing attacks within its staff, 486 staff were selected. The employees received an email requesting them to validate the user account such as login identity, addresses, and mobile number. The email sent to the was sent through a phishing website that looks like the institution's official website. The results of this exercise show that 31% (approximately 152) of staff clicked on the attached link of the received email. Moreover, 47.4% of the 152 staff provided their name while 93.1% provided their name and the password after clicking the link.