

ANALYSIS OF PHISHING VULNERABILITY AND
EMPLOYEE RESPONSE PATTERNS
IN SIMULATED EMAIL PHISHING CAMPAIGNS
USING A SECURITY AWARENESS TRAINING
PLATFORM

WONG LLI LLI

UNIVERSITI KEBANGSAAN MALAYSIA

ANALYSIS OF PHISHING VULNERABILITY AND EMPLOYEE RESPONSE
PATTERNS
IN SIMULATED EMAIL PHISHING CAMPAIGNS USING A SECURITY
AWARENESS TRAINING PLATFORM

WONG LLI LLI

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

FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2025

**ANALISIS KERENTANAN TERHADAP PHISHING DAN CORAK TINDAK
BALAS PEKERJA DALAM KEMPEN SIMULASI PHISHING E-MEL
MENGUNAKAN PLATFORM LATIHAN KESEDARAN KESELAMATAN**

WONG LLI LLI

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

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

DECLARATION

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

I acknowledge the use of AI (ChatGPT) was limited to supportive functions such as rewording and structuring content. All intellectual contributions, critical analysis, and final decision-making regarding content accuracy, and interpretation of results were conducted independently.

I affirm that this work complies with academic integrity standards and that all external sources are appropriately cited where applicable.

03 March 2025

WONG LLI LLI
P117802

ACKNOWLEDGEMENT

First and foremost, I would like to express my heartfelt thanks to Dr. Masnizah Binti Mohd, for having me under her supervision whose guidance, patience, and expertise have been invaluable throughout this journey. Her mentorship has not only steered me in the right direction, and late-evening brainstorming sessions, but also inspired me to push beyond my limits and strive for excellence.

I am also profoundly grateful to my family and friends for their unwavering support and encouragement, which kept me motivated during the most challenging phases of this project. A special note of thanks goes to my peers and colleagues who have shared ideas, constructive feedback, collaboration and camaraderie, making this journey both enriching and enjoyable.

Lastly, I extend my appreciation to all faculty, staff, and everyone who contributed to creating an environment conducive to learning and growth during my university time.

To every person, who contributed to this chapter of my life, you have my deepest appreciation. This journey has been more than an academic endeavour; it has been a joyful, humbling, and transformative experience. I am grateful beyond words! This project is not just a culmination of my efforts but a testament to the collective contributions of those around me.

ABSTRAK

Serangan phishing kekal sebagai ancaman keselamatan siber yang serius dan terus berkembang dengan mengeksploitasi kelemahan manusia untuk mendapatkan akses tanpa kebenaran kepada sistem yang sensitif. Kajian ini menyiasat tahap kerentanan pekerja terhadap serangan phishing serta corak tindak balas mereka dalam sebuah organisasi bersaiz sederhana dengan menggunakan *KnowBe4 Security Awareness Training Platform*, dengan maklumat organisasi dianonimkan bagi memastikan privasi. Walaupun teknologi keselamatan siber semakin maju, faktor manusia masih menjadi kelemahan utama dalam pertahanan terhadap ancaman ini, kerana pekerja sering menjadi mangsa akibat kurangnya kesedaran atau latihan, yang boleh membawa kepada kebocoran data dan pelanggaran keselamatan organisasi. Kajian ini bertujuan untuk menilai bagaimana faktor geografi mempengaruhi kerentanan terhadap serangan phishing dan keberkesanan latihan kesedaran siber, menganalisis corak tindak balas dalam simulasi phishing, termasuk interaksi e-mel, klik pautan, dan percubaan memasukkan data di pelbagai lokasi, serta mencadangkan strategi yang boleh dilaksanakan untuk meningkatkan keberkesanan program latihan kesedaran phishing dalam organisasi. Kajian ini menggunakan metodologi kuantitatif, menganalisis metrik seperti kadar klik, percubaan memasukkan data, dan kadar penyelesaian latihan, serta disokong oleh maklum balas kualitatif untuk memahami corak tingkah laku pengguna dan impak latihan. Hasil kajian menunjukkan bahawa latihan yang disasarkan dan disesuaikan secara geografi dapat mengurangkan kerentanan terhadap serangan phishing dengan ketara, dengan peningkatan ketara dalam kesedaran keselamatan siber dalam kalangan kumpulan berisiko tinggi. Selain itu, tingkah laku pelaporan juga menunjukkan peningkatan yang memberangsangkan, mengukuhkan keberkesanan modul latihan yang lebih interaktif dan adaptif. Kajian ini menyumbang kepada bidang keselamatan siber dengan membuktikan keberkesanan simulasi phishing berasaskan lokasi serta pendekatan latihan berstruktur dalam mengurangkan risiko serangan phishing. Selain itu, kajian ini turut menyediakan cadangan praktikal untuk mengintegrasikan platform seperti KnowBe4 ke dalam strategi keselamatan siber organisasi. Penemuan ini juga mencadangkan penambahbaikan dasar, termasuk pelaksanaan program latihan keselamatan siber wajib mengikut peranan serta simulasi phishing berkala, bagi memperkukuhkan kesedaran pekerja dan meningkatkan keselamatan organisasi secara keseluruhan.

ABSTRACT

Phishing attacks remain a significant and evolving cybersecurity threat, exploiting human vulnerabilities to gain unauthorized access to sensitive systems. This study investigates employee susceptibility to phishing and response patterns within a mid-sized organization using the KnowBe4 Security Awareness Training Platform, with organizational details anonymized for privacy. Despite advancements in cybersecurity technology, human factors remain the weakest link in defending against phishing threats, as employees often fall victim due to insufficient awareness or training, leading to data breaches and security compromises. This study aims to assess how geographical factors influence phishing susceptibility and training outcomes, analyze response patterns in phishing simulations—including email interactions, link clicks, and data entry attempts—across multiple regions, and propose actionable strategies for improving phishing awareness training. The study employs a quantitative methodology, analyzing metrics such as click-through rates, data entry attempts, and training completion rates, with qualitative feedback incorporated for deeper insights into behavioral trends and training effectiveness. Findings demonstrate that targeted, localized training significantly reduces phishing susceptibility, with phish-prone percentages decreasing after post-training and notable improvements among high-risk groups, such as Korean and Japanese employees. Reporting behavior also showed a substantial increase, reinforcing the effectiveness of adaptive training modules and region-specific education. This study contributes to the field by demonstrating the effectiveness of localized phishing simulations and gamified training approaches in mitigating phishing risks. It provides actionable recommendations for integrating platforms like KnowBe4 into organizational cybersecurity strategies and advocates for policy enhancements, such as mandatory role-specific training programs and periodic phishing simulations, to reinforce employee vigilance and strengthen overall cybersecurity posture.

TABLE OF CONTENTS

		Page
DECLARATION		iii
ACKNOWLEDGEMENT		iv
ABSTRAK		v
ABSTRACT		vi
TABLE OF CONTENTS		vii
LIST OF TABLES		xi
LIST OF ILLUSTRATIONS		xii
LIST OF ABBREVIATIONS		xiv
CHAPTER I	INTRODUCTION	
1.1	Research Background	1
1.2	Problem Statement	4
1.3	Research Question	6
	1.3.1 Employee Susceptibility and Geographical Influence	6
	1.3.2 Behavioural Patterns	6
	1.3.3 Training Program Effectiveness	6
1.4	Research Objectives	7
1.5	Research Scope	8
	1.5.1 Geographical Context	8
	1.5.2 Participants	8
	1.5.3 Phishing Simulations	8
	1.5.4 Awareness Training	9
	1.5.5 Metrics and Analysis	9
	1.5.6 Limitations	9
1.6	Significance of The Study	10
	1.6.1 Academic Contributions	10
	1.6.2 Practical Contributions	11
	1.6.3 Regional Relevance	11
	1.6.4 Long-Term Impact	12
1.7	Thesis Outline	13
	1.7.1 Chapter 1: Introduction	13
	1.7.2 Chapter 2: Literature Review	13
	1.7.3 Chapter 3: Methodology	13

1.7.4	Chapter 4: Results and Discussion	13
1.7.5	Chapter 5: Conclusion and Recommendations	14
CHAPTER II	LITERATURE REVIEW	
2.1	Introduction	15
2.2	Types of Phishing Emails	17
	2.2.1 Digital Phishing	18
	2.2.2 Physical Phishing	19
	2.2.3 Hybrid Techniques	19
2.3	Email Design	20
	2.3.1 Key Design Elements of Phishing Emails	20
	2.3.2 Psychological Triggers in Email Design	22
	2.3.3 Case Study: Email Template Design in the C1 2024 Campaign	23
	2.3.4 Case Study: Email Template Design in the C2 2024 Campaign	26
2.4	Security Assessment	30
	2.4.2 Tools for Security Assessment	32
2.5	Cybersecurity Awareness Training	33
	2.5.1 Tools Used in C1 and C2 2024 Campaign	34
	2.5.2 Benefits of the Proposed Approach	35
	2.5.3 Proposed Model	35
	2.5.4 Discussion	38
2.6	Conclusion	40
CHAPTER III	METHODOLOGY	
3.1	Introduction	41
3.2	Research Design	42
	3.2.1 Quantitative Methods	43
	3.2.2 Qualitative Methods	43
3.3	Workflow	44
	3.3.1 Phase 0: Preparation	44
	3.3.2 Phase 1: Configuration	46
	3.3.3 Phase 2: Execution	46
	3.3.4 Phase 3: Data Collection	46
	3.3.5 Phase 4: Data Analysis	47
	3.3.6 Functional Flow (Deceived Users)	47
3.4	KnowBe4 Platform Configuration Setup	48
	3.4.1 Email Design	48
	3.4.2 Body Design	49

	3.4.3	Target User Configuration	57
	3.4.4	Domain Whitelisting and Landing Pages	57
	3.4.5	Training Module Configuration	58
	3.4.6	Email Delivery and Monitoring	58
	3.4.7	Identify Deceived Users	59
3.5		Data Collection	60
	3.5.1	Metrics Collected	60
	3.5.2	Tools Used for Data Collection	61
	3.5.3	Data Validation	62
	3.5.4	Data Segmentation	62
3.6		Data Analysis	63
	3.6.1	Quantitative Analysis	63
	3.6.2	Qualitative Analysis	64
3.7		Ethical Considerations	65
CHAPTER IV RESULTS AND DISCUSSION			
4.1		Introduction	66
4.2		Results	66
	4.2.1	Campaign Overview	66
	4.2.2	Phishing Test Results	67
4.3		Awareness Training Results	74
	4.3.1	Training Campaign Overview	74
	4.3.2	Training Completion Rates	75
	4.3.3	Pre and Post Training Impact	76
	4.3.4	Feedback from Participants	79
4.4		Discussion	81
	4.4.1	Alignment with Literature	81
	4.4.2	Practical Implications	82
CHAPTER V CONCLUSION AND FUTURE WORKS			
5.1		Introduction	84
5.2		Discussion	84
	5.2.1	Awareness Training Impact	85
	5.2.2	Behavioural and Demographic Insights	86
5.3		Recommendations	87
	5.3.1	Tailored Awareness Training	87
	5.3.2	Enhanced Reporting Mechanisms	87
	5.3.3	Continuous Monitoring and Improvement	88
	5.3.4	Organizational Policy Enhancements	89
5.4		Limitations of the Study	89

5.4.1	Scope of Analysis	89
5.4.2	Single-Platform Dependency	90
5.4.3	Geographical Constraints	90
5.5	Future Research Directions	90
5.5.1	Multi-Vector Phishing Simulations	90
5.5.2	Long-Term Impact of Training	91
5.5.3	Cross-Industry Analysis	91
5.5.4	Cultural and Demographic Factors	91

REFERENCES

92

APPENDICES

Appendix A	HTML Code used to created C2 Phishing Email (English)	95
Appendix B	HTML code used to create C2 Data Entry LANDING page	99

LIBRARY FROM

LIST OF TABLES

Table No.		Page
Table 1.1	Research Question aligned with Research Objective	7
Table 2.1	Proposed Security Approach	35
Table 2.2	Research Gaps	36
Table 2.3	How the Proposed Model Addresses Research Gaps	39
Table 3.1	Gantt Chart Timeline	45
Table 3.2	Step to Identify Deceived User	59
Table 3.2	Step to Identify Non-Deceived User	59
Table 4.1	Campaign Period	67
Table 4.2	Phishing Campaign Participant Count	67
Table 4.3	C1 Phishing Campaign Results	67
Table 4.4	C2 Phishing Campaign Results	69
Table 4.5	Compare C1 and C2 Improvement	73
Table 4.6	Training Completion Rates	76
Table 4.7	Phish-Prone Percentage Comparison	77
Table 4.8	User Reporting Behaviour Pre and Post Training Comparison	78
Table 4.9	Findings for Proposed Model and Research Gaps	81

LIST OF ILLUSTRATIONS

Figure No.		Page
Figure 2.1	Types of Phishing Attacks	18
Figure 2.2	Email Preview- HR: Confirm your emergency contact information	23
Figure 2.3	Email Preview- Landing Page for HR Login Page	24
Figure 2.4	Email Preview-Final Landing Page for Simulated Phishing Test	25
Figure 2.5	Email Preview- Google: Password Security Alert	26
Figure 2.6	Email Preview- Landing Page for Google Login Page	28
Figure 2.7	Email Preview- Oops! Final Landing Page for Simulated Phishing Test	28
Figure 2.8	Methodology	31
Figure 2.9	Metrics for Evaluation	31
Figure 2.10	Challenges and Mitigation Strategies	36
Figure 3.1	Phases of Phishing Campaign	41
Figure 3.2	Deceived User Functional Flow	47
Figure 3.3	Non-Deceived User Functional Flow	48
Figure 3.4	Overview of Email Design Template created in KnowBe4	49
Figure 3.5	Design Phishing Email in Editor	50
Figure 3.6	Phishing Email (English)	50
Figure 3.7	Phishing Email (Chinese)	51
Figure 3.8	Phishing Email (Korean)	51
Figure 3.9	Phishing Email (Japanese)	52
Figure 3.10	Design for Data Entry Landing Page	52
Figure 3.11	Data Entry Landing Page design in HTML code	53
Figure 3.12	Data Entry Landing Page design with different language	53

Figure 3.13	Data Entry Landing Page after click on Check Passwords	54
Figure 3.14	Oops! Landing Page (English)	55
Figure 3.15	Customized Final Landing Page (Korean)	55
Figure 3.16	Training Notification Email Design	56
Figure 3.17	Training Reminder Email Design	56
Figure 4.1	C1 Data Entered (Failures)	68
Figure 4.2	C1 Data Entered by Department	68
Figure 4.3	Number of C1 Users Who Reported by Countries	69
Figure 4.4	C2 Data Entered (Failures)	70
Figure 4.5	C2 Data Entered by Department	70
Figure 4.6	Number of C2 Users Who Reported by Countries	71
Figure 4.7	Training Completion Rates for D1	75
Figure 4.8	Training Completion Status by Country	75
Figure 4.9	Survey Results	79

LIST OF ABBREVIATIONS

C1	Campaign 1
C2	Campaign 2
D1	Deceived 1 User
CN	Chinese
ENG	English
JPN	Japanese
KOR	Korean
IT	Information Technology
KnowBe4	KnowBe4 Security Awareness Training Platform
KPI	Key Performance Indicator
Phish-Prone %	Percentage of users susceptible to phishing attacks
SMS	Short Message Service
URL	Uniform Resource Locator
UAT	User Acceptance Test

CHAPTER I

INTRODUCTION

1.1 RESEARCH BACKGROUND

The increasing frequency and sophistication of cyber threats have made cybersecurity a critical priority for organizations worldwide, including Malaysia. Among these threats, phishing remains one of the most widespread and evolving attack vectors, exploiting psychological manipulation techniques—such as urgency, fear, and authority—to deceive individuals into divulging sensitive information like login credentials and financial data (Almomani, 2013) (Jampen, 2020) . In 2023, CyberSecurity Malaysia reported that phishing accounted for a significant proportion of the 20,000 cybersecurity incidents recorded, with government agencies and telecommunications being the most frequently targeted sectors (The Star, 2023).

The economic and reputational consequences of phishing are particularly severe in Malaysia, where sophisticated cybercriminal campaigns have targeted high-value sectors such as finance, telecommunications, and e-commerce. In Q3 2023, Malaysia ranked as the eighth most breached country globally, experiencing a 144% increase in leaked accounts compared to the previous quarter (Surfshark, 2023). Such alarming statistics highlight the urgent need for organizations to implement robust countermeasures to mitigate phishing risks and strengthen cybersecurity resilience.

To address these challenges, Malaysia has introduced cybersecurity awareness initiatives such as the CyberSAFE Program, which aims to educate individuals and organizations on recognizing and reporting phishing attacks (CyberSAFE Malaysia). Similarly, private sector organizations are increasingly adopting phishing simulation

and training platforms like KnowBe4, Cofense PhishMe, and Mimecast Awareness Training to enhance phishing awareness. KnowBe4, in particular, is widely used due to its multilingual capabilities and customizable phishing templates, making it well-suited for Malaysia's diverse workforce (Taylor, 2021).

However, despite the adoption of such security awareness measures, the effectiveness of phishing training varies across geographical regions and organizational environments. Studies suggest that cultural and regional factors influence employee susceptibility to phishing, particularly in societies where trust in authority figures is deeply ingrained (Nguyen, 2020). In Malaysia, phishing attacks often impersonate senior executives or government officials, exploiting hierarchical workplace dynamics to manipulate employees into compliance. Additionally, Malaysia's high smartphone penetration rate has expanded the phishing attack surface beyond emails to include mobile-based phishing (smishing) and fraudulent app-based scams (Cyber Security Malaysia, MyCERT Report - Cyber Incident Quarterly Summary Report - Q3 2024, 2024)

As a Managed Service Provider (MSP) and Security Consultant, my role is to assist the organizations in configuring, managing, and optimizing KnowBe4 phishing awareness training programs. This involves helping organizations familiarize themselves with the KnowBe4 platform, consulting on phishing email template design, managing the rollout of phishing and security training campaigns, and analysing simulation results to refine future awareness strategies.

For this research, the company specializes in the development and deployment of renewable energy solutions. Founded in 2010, the company has established itself as a leader in the renewable energy sector, focusing on solar and wind energy projects. Over the years, it has expanded its operations internationally, with a presence in over 20 countries. The study focuses on evaluating phishing susceptibility across multiple regions where employees communicate in English, Chinese, Japanese, and Korean,

providing insights into how regional cybersecurity behaviours influence phishing response rates.

By leveraging the KnowBe4 Security Awareness Training Platform, this study examines employee vulnerability to phishing within a multinational organizational context. By analysing key phishing simulation metrics, such as email open rates, link clicks, and data entry attempts, this research evaluates the effectiveness of region-specific security awareness training in reducing phishing susceptibility. The findings aim to provide actionable insights for improving phishing awareness programs, strengthening Malaysia's overall cybersecurity posture, and fostering a culture of digital resilience in organizations (Sheng, 2010)

LIBRARY FTSM

1.2 PROBLEM STATEMENT

Phishing attacks remain a persistent and growing threat to organizational security, exploiting human vulnerabilities to bypass even advanced cybersecurity defenses. In Malaysia, phishing is a leading cause of cybersecurity incidents, CyberSecurity Malaysia reporting that such attacks constituted a significant proportion of the 20,000 incidents recorded in 2023 (Cyber Security Malaysia, Annual Report, 2023) (Cyber Security Malaysia, Malaysia Cybersecurity Incident Report: Phishing and Social Engineering Trends, 2023) . Employees often represent the weakest link, unknowingly falling victim to phishing attempts due to insufficient training or limited awareness of phishing tactics (Parsons, Phishing for the truth: A scenario-based experiment of users' susceptibility to phishing, 2024)

While phishing and awareness campaign have proven effective in addressing phishing risks, their success depends heavily on the quality of implementation and sustained employee engagement (Taylor, 2021). Malaysian organizations face unique challenges related to cultural norms and technological trends. For instance, a high level of trust in authority figures increases the susceptibility of Malaysian employees to phishing emails impersonating senior executives or government officials (Nguyen, 2020). Additionally, Malaysia's high smartphone penetration rate has shifted phishing campaigns toward mobile platforms, introducing new vulnerabilities that many training programs fail to address (Cyber Security Malaysia, Malaysia Cybersecurity Incident Report: Phishing and Social Engineering Trends, 2023).

For this research I will examines employee vulnerability to phishing within (one) organizations with one of the branch located in Malaysia, focusing on the effectiveness of localized training programs delivered through the KnowBe4 platform. By evaluating metrics such as email open rates, link clicks, and data entry attempts, this research aims to provide actionable insights for improving phishing resilience and tailoring cybersecurity training to Malaysia's unique cultural and technological landscape. Variables such as job roles, prior exposure to cybersecurity training, and regional differences play significant roles in shaping phishing resilience (Vishwanath

A. H., 2011). Addressing these gaps is critical for optimizing security awareness training in Malaysia's organizational context.

LIBRARY FTSM

1.3 RESEARCH QUESTION

This research addresses the following questions:

1.3.1 Employee Susceptibility and Geographical Influence

How susceptible are employees to phishing attacks across different geographical regions, and how do regional factors impact phishing susceptibility and training outcomes? (Sheng, 2010) (Alseadoon, 2012)

1.3.2 Behavioural Patterns

What patterns emerge in employee responses to simulated phishing campaigns, including email interactions, link clicks, and data entry attempts? (Vishwanath A. H., 2011) (Halevi, Phishing, personality traits and Facebook, 2013)

1.3.3 Training Program Effectiveness

What improvements can be made to enhance the effectiveness of phishing awareness training programs, particularly for organizations operating in multiple regions? (Canfield, Training to mitigate phishing attacks, 2016) (Cyber Security Malaysia, Improving cybersecurity resilience: A roadmap for security awareness training in Malaysia, 2023)

1.4 RESEARCH OBJECTIVES

The objectives of this study are as follows:

1. To assess how demographic factors and language group differences influence phishing susceptibility and training outcomes (Sheng, 2010) (Alseadoon, 2012)
2. To analyse response patterns in phishing simulations, including email interactions, link clicks, and data entry attempts, across multiple language groups. (Vishwanath A. H., 2011) (Halevi, Phishing, personality traits and Facebook, 2013)
3. To propose actionable strategies for enhancing the design and delivery of phishing awareness training programs, with a focus on language-specific customization according to geographical

Table 1.1 Research Question aligned with Research Objective

Research Question	Research Objective
1. How susceptible are employees to phishing attacks across different geographical regions, and how do regional factors impact phishing susceptibility and training outcomes?	Objective 1: To assess how geographical factors influence phishing susceptibility and training outcomes in a multinational organization.
2. What patterns emerge in employee responses to simulated phishing campaigns, including email interactions, link clicks, and data entry attempts?	Objective 2: To analyse response patterns in phishing simulations, including email interactions, link clicks, and data entry attempts, across multiple geographical regions.
3. What improvements can be made to enhance the effectiveness of phishing awareness training programs, particularly for organizations operating in multiple regions?	Objective 3: To propose actionable strategies for enhancing the design and delivery of phishing awareness training programs, with a focus on region-specific customization and improving training effectiveness.

1.5 RESEARCH SCOPE

This study assesses phishing awareness training effectiveness within a multinational organization using the KnowBe4 Security Awareness Training Platform. The research examines how geographical factors influence phishing susceptibility and training outcomes, providing insights into regional differences in cybersecurity behaviour and awareness levels. To achieve this, the study utilizes a mixed-method approach, combining quantitative metrics and qualitative feedback to analyse phishing response patterns and training effectiveness. The scope includes the following areas:

1.5.1 Geographical Context

This study examines employee responses across multiple countries, evaluating how regional differences impact phishing susceptibility and training effectiveness. (Darwish, 2012)

1.5.2 Participants

Employees from diverse roles and departments within the organization are included, providing a representative sample based on job function, work environment, and IT literacy levels. (Shropshire, 2015). The study differentiates between office-based employees and store-based employees, recognizing that exposure to digital threats and cybersecurity training engagement may vary across these groups.

1.5.3 Phishing Simulations

Phishing campaigns are conducted using the KnowBe4 Security Awareness Training Platform, leveraging simulated phishing attacks and interactive training modules. The phishing emails used in this study mimic common cyberattack tactics, such as password-reset scams and executive impersonations, to assess baseline (preliminary checking) phishing susceptibility and behavioural patterns. (Jensen, 2017)

1.5.4 Awareness Training

Security awareness training is delivered through KnowBe4's interactive modules, which include gamified training and phishing simulations. (Canfield, Training to mitigate phishing attacks, 2016). The study evaluates training effectiveness by comparing pre-training and post-training performance, measuring improvements in phishing detection and response rates.

1.5.5 Metrics and Analysis

This research employs a combination of quantitative and qualitative methods:

1. Quantitative metrics include email open rates, link clicks, data entry attempts, and reporting rates, which help measure the overall phish-prone percentage. (Pattinson, 2012)
2. Qualitative feedback from employees is analysed to gain deeper insights into training engagement, user behaviour, and phishing awareness challenges.

1.5.6 Limitations

This study is limited to one multinational organization, which may impact the generalizability of findings to other industries or regions. The phishing simulations focus exclusively on email-based phishing, excluding other attack vectors such as smishing (SMS phishing) and vishing (voice phishing).

As the phishing simulations are conducted in a controlled environment, the study does not assess how employees react to real-world, high-pressure phishing attacks. (Cyber Security Malaysia, Challenges in cybersecurity awareness training and phishing simulations, 2023)

1.6 SIGNIFICANCE OF THE STUDY

This research holds significance in multiple dimensions, contributing to both theoretical advancements in phishing awareness and practical cybersecurity improvements for organizations. By evaluating phishing susceptibility and training effectiveness across multiple geographical regions, this study provides valuable insights into regional cybersecurity behaviours, training engagement, and phishing response patterns.

1.6.1 Academic Contributions

a. Expanding Literature on Phishing Awareness

This study enriches existing research on phishing awareness training by analysing the impact of regional cybersecurity behaviours on training outcomes, an area that remains underexplored in phishing mitigation studies. By examining how geographical factors influence phishing susceptibility, this research contributes a new perspective to cybersecurity training models and risk assessment methodologies.

b. Behavioural Insights

Through empirical analysis of employee interactions with phishing simulations, this study provides data-driven insights into human behaviour when exposed to phishing threats. These findings enhance existing social engineering models by identifying key factors influencing phishing susceptibility and reporting behaviours in different organizational environments.

1.6.2 Practical Contributions

a. Improving Organizational Resilience:

The findings offer actionable strategies to reduce phishing susceptibility through region-specific cybersecurity awareness training. Organizations can apply these insights to refine training programs and strengthen their overall security posture by targeting high-risk employee groups more effectively.

b. Enhancing Awareness Training:

This study evaluates the effectiveness of KnowBe4's phishing simulation and training modules, providing practical insights for improving future phishing awareness initiatives. The research findings support customized training strategies, ensuring that organizations tailor phishing education programs to regional cybersecurity challenges rather than adopting a one-size-fits-all approach.

1.6.3 Regional Relevance

a. Addressing Malaysia-Specific Challenges

It supports national efforts, such as the CyberSAFE Program, by providing data-driven insights can guide policymaking and organizational practices. As a Managed Service Provider and Security Consultant, this study provides practical recommendations for improving KnowBe4 training implementations in multinational organizations. Findings from this research can assist security consultants, IT security teams, and managed security providers in designing more effective phishing awareness programs based on regional cybersecurity risks. While the study includes Malaysia, it also applies to other geographical regions, providing insights into regional cybersecurity behaviours and phishing susceptibility patterns. The research findings can support governmental and corporate cybersecurity awareness initiatives, reinforcing phishing resilience strategies across Asia and beyond.

b. Contributing to Asia's Cybersecurity Landscape

With phishing being a pervasive threat across the region, this study's findings can serve as a model for similar initiatives in other Asian countries with comparable technological landscapes. Organizations using phishing simulation platforms can leverage this study to improve employee engagement, enhance phishing reporting mechanisms, and optimize training effectiveness. The findings provide a foundation for policy improvements, emphasizing the need for mandatory, region-specific cybersecurity awareness training programs. The findings can be used as a model for cybersecurity professionals, training platforms, and policymakers seeking to enhance phishing awareness strategies globally.

1.6.4 Long-Term Impact**a. Reducing Organizational Risk**

By identifying weaknesses in current training programs in the organization and proposing improvements, the research aims to reduce the risk of email phishing-related data breaches, financial losses, and reputational damage.

b. Advancing Cybersecurity Practices

The research supports the development of proactive cybersecurity strategies, emphasizing the importance of human factors alongside technological defences as conducted within the Malaysia organization. The findings encourage continuous security awareness training, ensuring that organizations remain adaptable in mitigating evolving phishing threats.

1.7 THESIS OUTLINE

1.7.1 Chapter 1: Introduction

This chapter introduces the research topic, providing an overview of the background, problem statement, research questions, objectives, scope, significance, and thesis outline. It establishes the foundation for the study by emphasizing the importance of cybersecurity awareness and phishing mitigation strategies within an organizational context, with a particular focus on regional cybersecurity behaviours in Malaysia.

1.7.2 Chapter 2: Literature Review

The literature review explores existing research on phishing attacks, user behaviour, and security awareness training effectiveness. It examines the role of phishing simulation platforms, including KnowBe4, in mitigating cybersecurity risks. Additionally, this chapter discusses geographical influences, phishing susceptibility factors, and training engagement levels while identifying gaps that this study aims to address.

1.7.3 Chapter 3: Methodology

This chapter details the research design, including the experimental setup of phishing simulations and training programs using the KnowBe4 platform. It explains participant selection criteria, the structure of phishing email campaigns, training interventions, and data collection techniques. Furthermore, it outlines the analytical methods used to evaluate employee phishing susceptibility and the effectiveness of cybersecurity training programs.

1.7.4 Chapter 4: Results and Discussion

The results chapter presents findings from phishing simulation campaigns and awareness training (C2 2024). It provides an analysis of employee responses, regional differences, and cybersecurity awareness outcomes. Key insights include phish-prone

percentages, reporting rates, and behavioural patterns. The discussion interprets these findings in relation to existing cybersecurity literature and training methodologies.

1.7.5 Chapter 5: Conclusion and Recommendations

The final chapter summarizes research findings, practical implications, and theoretical contributions. It offers recommendations for optimizing phishing awareness training programs, improving cybersecurity resilience, and addressing limitations in training approaches. Additionally, it discusses the study's constraints and outlines potential directions for future research on phishing awareness and cybersecurity training frameworks.

LIBRARY ETSM

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

Phishing remains one of the most pervasive cybersecurity threats, contributing to over 80% of data breaches globally (Verizon, 2023). These attacks exploit human vulnerabilities through deceptive tactics, such as impersonating trusted entities and manipulating users into sharing sensitive information (Almomani, 2013) (Jampen, 2020). Despite advancements in cybersecurity technologies, phishing continues to evolve, leveraging sophisticated strategies to bypass technical defences (Parsons, 2024). Phishing for the truth: A scenario-based experiment of users' susceptibility to phishing, 2024)

Extensive research has focused on understanding phishing techniques, factors influencing user susceptibility, and the effectiveness of security awareness training (Sheng, 2010). However, significant research gaps remain, particularly regarding how regional cybersecurity behaviours and organizational security cultures impact phishing awareness and training effectiveness (Vishwanath A. H., 2011). Studies have not fully explored how phishing training outcomes vary across different geographical locations and the role of localized security training strategies in mitigating phishing risks (Nguyen, 2020).

In response to these challenges, phishing simulation and awareness training platforms such as KnowBe4, Cofense PhishMe, and Mimecast Awareness Training have emerged as critical tools for enhancing employee resilience to phishing threats

(Canfield, Training to mitigate phishing attacks, 2016). While these platforms offer interactive training modules and real-world phishing simulations, regional cybersecurity behaviours and language-specific phishing risks may influence their effectiveness.

This chapter reviews existing research to provide a foundation for the methodology and analysis in subsequent chapters. The literature review is structured around four key areas:

1. **Phishing Threats and Attack Strategies:** Analysing the techniques employed by attackers to deceive users and evade detection.
2. **Human Factors in Phishing Susceptibility:** Analysing how regional cybersecurity behaviours and organizational policies influence phishing response patterns.
3. **Effectiveness of Security Awareness Training:** Evaluating the role of phishing simulation platforms (e.g., KnowBe4, Cofense PhishMe, Mimecast Awareness Training) in reducing phishing susceptibility.
4. **Gaps and Challenges in Current Research:** Identifying areas where further exploration is needed, such as the impact of regional security cultures on phishing defence strategies.

By critically reviewing the existing research, this study highlights the need for tailored region-specific training approaches and the role of phishing simulations in building a resilient cybersecurity culture within multinational organizations.

2.2 TYPES OF PHISHING EMAILS

Phishing attacks remain a persistent and evolving cybersecurity threat, continuously adapting to exploit human vulnerabilities and bypass security defences (Jakobsson M. &, 2016). These attacks often rely on psychological manipulation, deception, and social engineering techniques to trick individuals into disclosing sensitive credentials, financial details, or organizational data (Hong, 2012). Attackers use various deceptive tactics, generally can be grouped these into three main types: digital phishing, physical phishing, and hybrid technique. These classifications (Abbasi, 2010) are illustrated in Figure 2.1, providing a structured overview of the different phishing attack methodologies.

Understanding these types is key to recognizing how phishing works, the damage it can cause, and how to protect against it. It is essential for identifying the methodologies used by attackers, assessing their impact, and implementing effective countermeasures. This section also breaks down each category, sharing practical examples, key strategies used by attackers, and what these mean for keeping organizations secure.

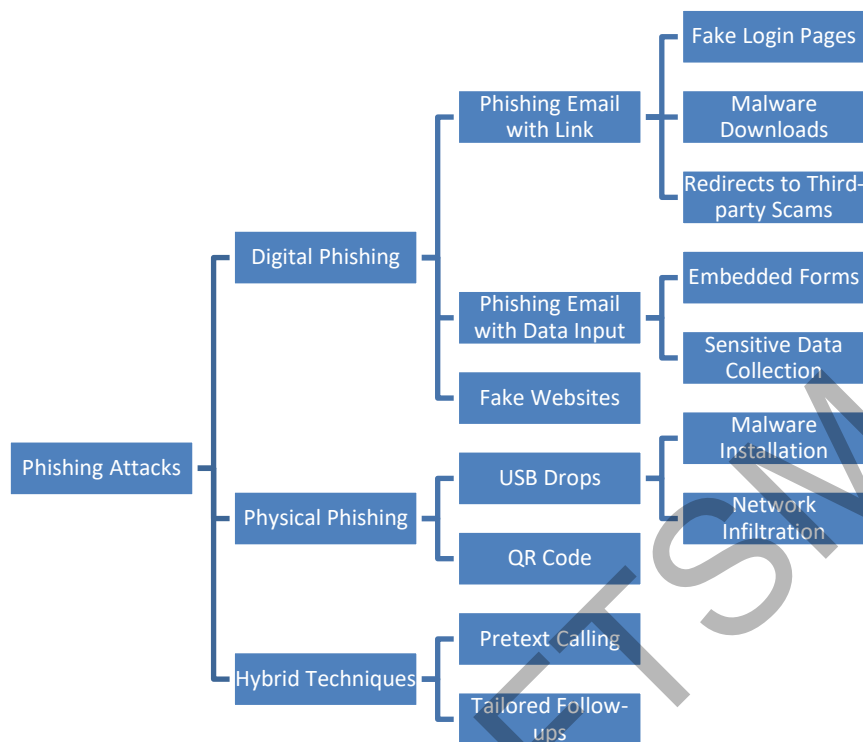


Figure 2.1 Types of Phishing Attacks

Source: (Jakobsson M. &, 2016) (Parsons, Phishing for the truth: A scenario-based experiment of users' susceptibility to phishing, 2014) (Chiew, 2018) (Gupta, 2018)

2.2.1 Digital Phishing

Digital phishing is the most common and widely used technique to exploiting electronic communication channels, such as email, websites, messaging applications. These attacks deceive users into revealing sensitive information, and typically executed in three key forms:

1. **Phishing Emails with Links:** Include links directing users to fake login pages, malicious downloads, or third-party scam websites. (Abbasi, 2010)
2. **Phishing Emails with Embedded Forms:** Contain forms embedded directly in the email to collect sensitive data, such as login credentials or financial information. (Fette, 2007)
3. **Fake Websites:** These mimic legitimate sites to deceive users into providing personal information, using tactics like domain spoofing to appear authentic. (Thomas, 2011)

2.2.2 Physical Phishing

Physical phishing involves tangible tactics designed to exploit trust or curiosity, often requiring the victim to interact with a physical object. These methods bypass traditional digital defences, making them a significant security concern.

1. USB Drops: Involves leaving USB devices in accessible public areas, such as parking lots or lobbies to entice users into plugging them into their computers, often leading to malware installation or network infiltration. (Bursztein, 2016)
2. QR Code: QR codes are embedded in printed materials, such as posters or flyers, claiming to provide useful information to deceive victims into scan and redirect users visiting fraudulent websites or initiates unauthorized actions, such as stealing credentials. (Kirchner, 2019)

2.2.3 Hybrid Techniques

Hybrid techniques combine digital and physical tactics, often incorporating social engineering to enhance their effectiveness.

1. Pretext Calling: Attackers impersonate legitimate entities (e.g., IT support) to gain sensitive information (Vishwanath A. H., 2011)
2. Tailored Follow-Ups: Combine phishing emails with personalized calls or messages to reinforce deception. (Halevi, Phishing, personality traits, and Facebook, 2013)

2.3 EMAIL DESIGN

Phishing emails are carefully crafted to deceive recipients into believing they are legitimate, mimicking trusted entities or employing urgent language to manipulate user behaviour. Effective phishing email design combines psychological manipulation with technical elements to maximize the likelihood of user engagement. The key aspects of phishing email design, including visual elements, language use, and tactics employed to bypass security measures is explained in this section.

2.3.1 Key Design Elements of Phishing Emails

a. Sender Spoofing

Phishing emails often use spoofed sender addresses to appear as though they originate from trusted organizations. Users may not scrutinize the sender's address, especially under time pressure

- i. **Slight variations in domain names (e.g., support@bank-secure.com instead of support@bank.com).**
- ii. **Use of generic sender names, such as “Security Team” or “Admin” or “HR”**

b. Subject Lines

The subject line is designed with psychological triggers, fear, create urgency, curiosity drive users to open the email or grab attention.

- i. **“Action Required: Your Account Will Be Suspended”**
- ii. **“Unusual Login Attempt Detected”**

c. Body Content

The content of phishing emails often mimics legitimate communication, combining urgency with professional language and layout.

- i. A brief explanation of the issue (e.g., “Your account has been compromised”).**
- ii. A call-to-action (e.g., “Click here to reset your password”).**

Use of logos and branding to enhance credibility.

d. Hyperlinks

Links within phishing emails often redirect users to malicious websites.

- i. Displaying fake URLs that look legitimate (e.g., <https://www.bank-security.com>).**
- ii. Hiding malicious URLs behind text like “Click Here” or buttons.**

e. Attachments

Phishing emails sometimes include malicious attachments disguised as invoices, reports, or forms. Common File Types: PDFs, Word documents with macros, and ZIP files containing malware.