ADDIS ABABA UNIVERSITY

SCHOOL OF COMMERCE

DEPARTMENT OF BUSINESS ADMINISTRATION & INFORMATION SYSTEMS

IMPACT OF SECURITY AWARENESS PROGRAM ON EMPLOYEE PHISHING RESILIENCE: A CASE STUDY AT COMMERCIAL BANK OF ETHIOPIA

By: Daniel Kelemework Admasu

Advisor: Meshesha Legesse (PhD)

A Thesis Submitted to in Partial Fulfillment of the Requirements for the Degree of Master of Business Information Systems

June, 2025

Addis Ababa, Ethiopia

DECLARATION

I, the undersigned declare that this research thesis entitled "**Impact of security awareness program on employee phishing resilience: a case study at Commercial Bank of Ethiopia**" is my original work, prepared under the guidance of Meshesha Legesse (PhD). All sources of materials used for the research have been duly acknowledged. I further confirm that the research has not been submitted either part or in full to any other higher learning institutions for the purpose of earing any degree.

Daniel Kelemework	_____	_____
Name	Signature	Date

STATEMENT OF CERTIFICATION

This is to certify that, this research thesis entitled "**Impact of security awareness program on employee phishing resilience: a case study at Commercial Bank of Ethiopia**" undertaken by Daniel Kelemework Admasu in partial fulfillment of the requirements for Master of Science in Business Information Systems at Addis Ababa University School of Commerce is an original work and not submitted earlier for any Degree either at this university or any other university.

_____

Meshesha Legesse (PhD)
Research Advisor

ADDIS ABABA UNIVERSITY
COLLEGE OF BUSINESS AND ECONOMICS
SCHOOL OF COMMERCE
BUSINESS INFORMATION SYSTEMS PROGRAM

Impact of Security Awareness Program on Employee Phishing Resilience: A Case Study at Commercial Bank of Ethiopia

By: Daniel Kelemework Admasu

Approval of Examiners

Meshesha Legesse (PhD)

Advisor Signature

_____

Internal Examiner	Signature	Date
_____	_____	_____

External Examiner	Signature	Date
_____	_____	_____

ACKNOWLEDGEMENT

I would like to begin by expressing my deepest gratitude to the Almighty God for granting me the strength, perseverance, and wisdom to undertake and complete this research study. Without His guidance, this achievement would not have been possible.

I am profoundly grateful to my advisor, **Dr. Meshesha Legesse**, for his invaluable guidance, insightful feedback, and unwavering support throughout this research journey. His expertise and encouragement have been instrumental in refining this study and ensuring its academic integrity.

My sincere appreciation extends to the employees of the Commercial Bank of Ethiopia (CBE) who contributed to this research through data collection and shared insights. Their cooperation and dedication were vital to the empirical foundation of this work.

I also extend my sincere appreciation to the scholars and researchers whose work has provided the foundation for this study. Their contributions to the field of information security have been a source of inspiration and direction.

Finally, I thank my family, friends, and colleagues for their encouragement and understanding during this demanding yet rewarding process.

ABSTRACT

This study investigates the effectiveness of security awareness training and the role of Protection Motivation Theory (PMT) constructs in shaping phishing resilience among employees of the Commercial Bank of Ethiopia. Despite technological protections, phishing remains a significant threat to organizations due to its psychological exploitation of human vulnerabilities. A quantitative approach was employed using structured questionnaires and organizational phishing report data from 396 randomly selected employees. Descriptive statistics, correlation, reliability testing, exploratory factor analysis (EFA), and multiple regression analyses were conducted using SPSS. The findings reveal that self-efficacy, response efficacy, response cost, and participation in security training significantly predict phishing resilience. Among these self-efficacy was the strongest contributor emphasizing the importance of users' confidence in avoiding phishing threats. In contrast, perceived threat severity and threat vulnerability were not statistically significant. Moderation analysis showed that job role significantly influenced the relationship between training and phishing resilience, with non-technical staff who participated in security awareness program showed more phishing resilience. This research highlights the need for training programs to focus not only on threat awareness but also on building user confidence and practical coping strategies. The study contributes to the application of PMT in cybersecurity and provides actionable recommendations for improving phishing awareness interventions in the banking sector in Ethiopia.

Keywords: Phishing, Security Awareness Program, Information Security, Security, Protection Motivation Theory (PMT), Cybersecurity, Employee Behavior.

LIST OF ABBREVIATIONS & ACRONYMS

- **CBE** - Commercial Bank of Ethiopia
- **SETA** - Security Education, Training, and Awareness
- **TPB** - Theory of Planned Behavior
- **HAIS-Q** - Human Aspects of Information Security Questionnaire
- **IT** - Information Technology
- **ISP** - Information Security Policy
- **VPN** - Virtual Private Network
- **SNS** - Social Networking Sites
- **USB** - Universal Serial Bus
- **ERP** - Enterprise Resource Planning
- **CRM** - Customer Relationship Management
- **SPSS** - Statistical Package for the Social Sciences
- **CISA** - Cybersecurity and Infrastructure Security Agency

LIST OF FIGURES

LIST OF TABLES

Table of Contents

Chapter One

Introduction

1.1. Research Background

In this interconnected digital age the banking sector is moving to information technology (IT) enabled services. Besides its benefits, this incremented dependency on IT comes with increasing cybersecurity threats particularly phishing attacks. The financial sector is highly exposed to cyber risks with nearly one-fifth of all cyber incidents affecting financial firms (IMF, 2024). As the largest state owned commercial bank in Ethiopia, the Commercial Bank of Ethiopia (CBE) manages a huge amounts of sensitive financial data, making it a prime target for sophisticated spear phishing attacks. Phishing is a deceptive practice where attackers impersonate trusted entities to steal sensitive data has surged in sophistication (Hadlington, 2018). Despite investments in technical safeguards like email filters, human vulnerability remains a critical weakness, with studies indicating that 90% of breaches originate from social engineering tactics (Verizon, 2023). To combat this and to foster phishing resilience among employees organizations deploy security awareness programs. Phishing resilience is employees' ability to detect, avoid, and report phishing attempts (Jampen et al., 2020). Security awareness programs are critical defenses against phishing, yet their effectiveness varies across organizational contexts. While some studies show employees' improved phishing detection post-training (Caputo et al., 2014), challenges like skill decay and overconfidence persist (Halevi et al., 2015). In developing economies, cyber risks are worsened by rapid digital transformation that outpaces security preparedness. The accelerated adoption of digital financial services often occurs without adequate investments in cybersecurity infrastructure and awareness program. This study investigates how security awareness programs at CBE influence phishing resilience, bridging a gap in context-specific research within Ethiopia's financial sector.

Information security is now the most crucial factor for organizations since cybersecurity risk is growing especially for the financial sector where huge volumes of sensitive customer data and monetary transactions are processed. Guaranteeing a strong security measure is vital for maintaining trust, protecting digital assets, and complying with regulatory requirements. Meanwhile, the strides in the development of cybersecurity tools are undermined by human error, which continues to be the main security weakness in the area of information security. Employees' non-compliance with security policies continues to be a significant risk factor, as

security breaches often result from poor security practices, negligence, or lack of awareness (Whitman & Mattord, 2018).

In turn, organizations introduce the Security awareness program to enhance the understanding of the security policies and foster compliance among the employees. Security awareness programs are designed to increase the knowledge of employees regarding security threats, security best practices, and the importance of following security protocols to prevent unauthorized access, data breaches, and cyber threats (Parsons et al., 2014). Compliance with information security policies ensures that employees adhere to established protocols, reducing security incidents and strengthening an organization's overall security posture (Ifinedo, 2012). Despite the widespread implementation of Security awareness programs, their effectiveness in improving employees' phishing resilience remains an area requiring further study. This study examines the relationship between SA programs and employees' phishing resilience at the Commercial Bank of Ethiopia (CBE) using the Protection Motivation Theory (PMT) (Rogers, 1975), which identifies three key psychological factors: perceived vulnerability to threats, self-efficacy in identifying phishing, and response cost assessments. The findings will provide insights into the strengths and limitations of existing SA initiatives and offer recommendations for improving phishing resilience within financial institutions.

1.2. Background of the Company

The Commercial Bank of Ethiopia (CBE) is the first and largest bank in Ethiopia established in 1942. CBE is a state-owned bank which is a key player of the economic development in the country providing banking services ranging from deposit mobilization to credit provisioning and foreign exchange operations also different types of digital banking services. CBE has more than 1900 branches and reaches more than 40 million account holders, 37 million Mobile Banking users and another 17 million CBE Birr users making it a cornerstone of Ethiopia's banking sector (CBE, 2024). The bank has been an early mover to leverage cutting edge technologies including mobile banking, internet banking, and card banking services, positioning itself as a leader in Ethiopia's transition to a digital economy. More than 70% of the bank's transactions are happening on digital banking services (CBE, 2024).

In recent years, CBE has made digital transformation a strategic priority, implementing cutting-edge technology to update its infrastructure and digital services like card banking, mobile wallets, and internet and mobile banking to improve its service delivery. In addition to its digital services, the bank has also digitized its internal business processes by deploying enterprise solutions such as ERP, CRM, Microsoft Exchange and IT help desk system. This

rapid digitization offers huge benefits, such as process efficiency, cost saving, increased accessibility and convenience for customers, but it has also introduced cybersecurity challenges. This increased use of technology has positioned CBE as a key target for many different cyber threats, especially those of an insider nature. To tackle the growing phishing threats CBE has developed an information security policy and implemented SA programs as part of its comprehensive information systems security strategy. These programs aim to enhance employee awareness, promote secure behaviors, and strengthen resilience against phishing cyber threats. However, the effectiveness of these initiatives in influencing employees' phishing resilience remains underexplored, necessitating this study.

1.3. Statement of the Problem

The growing cybersecurity threats continue to create significant risks to financial institutions. One of the key challenges in ensuring security is the human factor and phishing is one of the most common cyber threats today because it exploits human psychology rather than technical vulnerabilities (Caputo et al., 2014). Phishing is especially dangerous due to its personalized and deceptive nature which makes it difficult for users to detect and resist (Williams & Joinson, 2020). Despite the huge investments in technological cybersecurity defenses, organizations continue to face breaches due to employees falling victim to highly targeted phishing attacks. The main challenge is the human factor which relates to employees' awareness, motivation and confidence to identify and report phishing emails effectively. Eventhough security awareness programs are implemented widely by organizations to address the human factor challenges, their effectiveness varies. Many security awareness programs are generic and one time sessions that do not reinforce long-term behavioral change (Floderus & Rosenholm, 2019). Additionally, many users often overestimate their ability to detect phishing attempts and this overconfidence create a gap between perceived and actual security competence (Halevi et al., 2015). To address this gap many researchers have proposed the use of Protection Motivation Theory (PMT) as a theoretical framework to understand user's security behavior focusing on constructs threat severity, threat vulnerability, response efficacy, self-efficacy, and response cost (Rogers, 1983; Ifinedo, 2012). This PMT has been applied in various cybersecurity contexts, but there is limited research integrating these constructs to assess phishing resilience, particularly in Ethiopian banking institutions. Moreover, phishing resilience has not been adequately measured using a comprehensive model that includes both phychological and behavioral data. Furthermore, studies lack attention to how demographic factors (such as age, gender, and job role) may influence the effectiveness of training and the adoption of secure

practices. Therefore, this study seeks to address these gaps by evaluating the influence of PMT constructs and security awareness training on employees' phishing resilience, while also examining the moderating effects of demographic variables. The aim is to provide evidence-based recommendations for improving the design and targeting of security awareness programs in Ethiopia banking sector.

1.4. Research Objective

1.4.1 General Objective

The general objective of this study is to evaluate the impact of security awareness program and psychological factors adopted from PMT (threat severity, threat vulnerability, self-efficacy, response efficacy and response cost) on employees' phishing resilience at the Commercial Bank of Ethiopia (CBE).

1.4.2 Specific Objective

To achieve the general objective and to answer the research questions, the following specific objectives are defined for this research:

1. To assess whether employees participated in security awareness training have better phishing resilience.
2. To examine how PMT factors (threat severity, threat vulnerability, self-efficacy, response efficacy and response cost) influence employees' phishing resilience behaviour.
3. To explore the role of demographic factors (age, gender, job role) in moderating the relationship between training participation and phishing resilience.

1.5. Significance of the Study

The study on impact of security awareness programs on employees' phishing resilience focusing on the Commercial Bank of Ethiopia (CBE) has important contributions at theoretical, practical, and societal levels.

Theoretical Contributions

This research expands the application of the Protection Motivation Theory (PMT) in information security studies by providing empirical evidence on how security awareness programs influence employees' security behaviors specifically to employees' phishing resilience. While previous studies have examined generic phishing awareness (Sheng et al., 2010), this research specifically investigates how threat vulnerability, self-efficacy, and response cost influence employees' ability to detect targeted spear phishing attacks. By empirically testing PMT's applicability to spear phishing, the study contributes to behavioral

cybersecurity theories and provides a framework for future research on motivation-based training interventions.

Practical Contribution

For CBE and similar financial institutions, this study provides actionable insights into optimizing security awareness programs to enhance employee performance on identifying phishing emails. The findings can inform policy revisions, training enhancements, and targeted awareness campaigns to strengthen overall phishing resilience.

Social Contribution

As Ethiopia's largest bank, CBE's phishing resilience directly impacts millions of customers. So, by improving security awareness sand phishing resilience, this study contributes to protecting customer data, maintaining trust, and ensuring the stability of the banking sector.

1.6. Scope of the Study

This study evaluates the effectiveness of Security awareness training programs in improving employees' phishing resilience at the Commercial Bank of Ethiopia (CBE) with a focus on the role of Protection Motivation Theory (PMT) constructs (threat vulnerability, self-efficacy, and response cost). The scope is defined by the following dimensions:

Context: The research examines security awareness program within the Commercial Bank of Ethiopia, a leading financial institution managing massive customer data and critical financial operations. In particular, the context of this study is relevant because of CBEs' significant role in Ethiopia's financial sector and exposure to cybersecurity risks.

Subject Area: The study assesses the impact of security awareness program on employees phishing resilience and how PMT factors (threat severity, threat vulnerability, response efficacy, self-efficacy, response cost) influence employees behavior.

Participants: The primary participants are employees from different roles, departments, and experience level within CBE ensuring a comprehensive assessment of phishing resilience across the organization.

Geographical Focus: The study is limited to CBE's head office and selected branches in Ethiopia although the findings may have broader implications for similar financial institutions.

Time Frame: The study evaluates security awareness program implemented by CBE during the past one year to ensure the relevance of the data collected.

Thematic Scope: The study investigates the effectiveness of security awareness programs in enhancing employees phishing resilience, behavioral outcomes (detection accuracy, reporting habits), and psychological drivers (PMT constructs) behind security compliance.

Exclusions: The study does not examine broader cybersecurity measures, such as technical defenses or infrastructure improvements.

1.7. Limitation of the Study

This study provides valuable insights into the impact of security awareness program on employees' phishing resilience at CBE and the following are the limitations of the study that must be acknowledged:

Generalizability

As the study is focused only on CBE and its findings may not be entirely applicable to other financial institutions or industries. The difference in security awareness program maturity, organizational culture, policies, and security infrastructures across institutions potentially limits broader applicability.

Self-reported Data

Some measures of the study such as self-efficacy and threat vulnerability rely on self-reported responses which may be subject to bias such as overconfidence or social desirability effects. Actual behavior such as clicking on phishing links in real-world scenarios may differ from self-reported intentions or test performance.

Despite these limitations, the study provides valuable insights into the impact of security awareness programs on employees' phishing resilience at CBE. The findings are intended to inform practical improvements within the bank and serve as a foundation for further research in similar contexts.

1.8. Definition of Terms

To provide a foundational understanding of the study's key concepts and ensure consistency in the interpretation of findings, key terms used in this study are defined as follows:

Phishing resilience: Employee's ability to identify phishing emails, avoid clicking on malicious links or attachments, and report suspicious emails promptly. In this study, phishing resilience is measured using both self-reported behavior and organizational phishing report data.

Security Awareness Training: Organizational efforts designed to educate employees about cybersecurity threats including how to recognize and respond to phishing emails. These programs may include classroom workshops, phishing simulations, or online modules.

Protection Motivation Theory (PMT): A psychological framework that explains individuals' motivation to engage in protective behavior in response to perceived threats. The model

includes threat appraisal (threat severity, threat vulnerability) and coping appraisal (self-efficacy, response efficacy, response costs) constructs.

Threat Severity: The perceived seriousness of the consequences that would result from a phishing attack. Higher perceived severity is expected to motivate protective behavior.

Threat Vulnerability: The perceived likelihood or personal susceptibility to experiencing a phishing attack. Employees who feel more vulnerable are expected to adopt more secure behavior.

Response Efficacy: The belief that recommended protective actions like reporting or verifying emails are effective in preventing harm from phishing.

Self-Efficacy: An individual's confidence in their own ability to recognize and handle phishing emails effectively.

Response Cost: The perceived inconvenience, time, or effort required to perform protective behaviors (e.g., verifying emails, reporting suspicious email). Higher perceived response costs may discourage action.

Moderating Variable: A variable that influences the strength or direction of the relationship between independent and dependent variables. In this study, demographic factors such as age, gender, and job role are examined as moderators.

Actual Phishing Behavior: Objective behavioral outcomes derived from organizational phishing test reports including whether employees clicked on or reported phishing emails.

1.9. Organization of the Study

This study is divided into five chapters each covering an essential element of the research on impact of security awareness programs on employees' phishing resilience at the case study bank. This structure allows to provide a logical flow from the research background to the analysis and findings. Below is the organization of the thesis:

Chapter One: Provides an introduction to the research, including the background, problem statement, research objectives, scope, limitations, and definitions of key terms.

Chapter Two: Reviews relevant literature on information security, phishing, phishing resilience, SETA programs, and theoretical frameworks such as the Protection Motivation Theory (PMT).

Chapter Three: Outlines the research methodology, including research design, data collection methods, sampling techniques, and data analysis procedures.

Chapter Four: Presents the findings and analysis of the study based on the collected data.

Chapter Five: Discusses the results, draws conclusions, and provides recommendations for improving security awareness programs and employee phishing resilience within CBE.

Chapter Two

Literature Review

This chapter provides a comprehensive review of literature related to phishing resilience, security awareness programs, and the PMT. The review explores key theoretical foundations and empirical studies to establish a framework for understanding how security awareness programs influence employees' ability to detect and respond to spear phishing attacks. The chapter also examines the role of PMT constructs in predicting and shaping employees' phishing resilience.

2.1. Information Security

Information security refers to the practices and processes designed to protect information systems from unauthorized access, disclosure, modification, or destruction (Secfix, 2024). The primary objectives of information security are ensuring the confidentiality, integrity, and availability of data (Saeckel, 2022). As financial institutions increasingly rely on digital platforms for service delivery, the need for strong information security measures has become more critical than ever. According to (Whitman & Mattord, 2017,p.11), information security includes the broad areas of information security management including policy, computer security, data security, and network security to ensure the confidentiality, integrity, and availability.

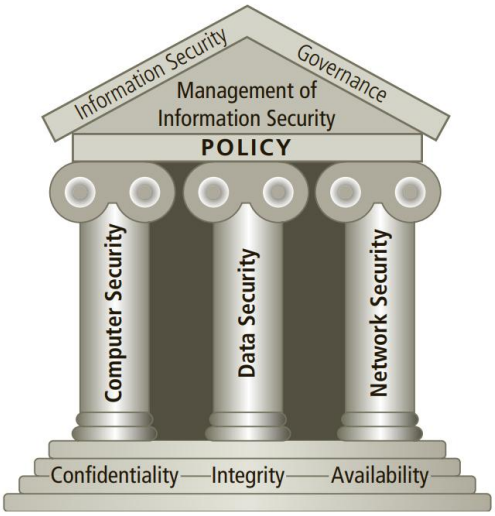


Figure 1 Components of Information Security (Whitman & Mattord, 2017,p.11)

The digitalization of financial services has exposed institutions to various security threats, including cyberattacks, data breaches, and phishing scams. Cybercriminals exploit vulnerabilities within organizations to gain unauthorized access to sensitive data, often

resulting in financial losses and reputational damage (Ifinedo, 2012). Employees play a significant role in preventing security breaches, making awareness and compliance essential components of an effective security strategy.

Information security involves safeguarding systems, networks, and data from both external and internal threats, but its effectiveness heavily depends on addressing human factors. Research underscores that addressing human errors effectively involves the implementation of security awareness programs which bridge the gap between cybersecurity policies and employee behavior (Hadlington, 2018). These programs focus on the human aspects of cybersecurity by raising awareness, encouraging compliance, and promoting secure practices (Alshaikh, 2020).

2.2. **Phishing**

Phishing is one of the most common type of social engineering technique that compels an email recipient to perform an action beneficial to the attacker (e.g. clicking a link to a fraudulent link or downloading a malicious attachment) (Nieles, Dempsey and Pillitteri, 2017). It is a deceptive practice where attackers impersonate trusted entities to steal sensitive data such as login credentials or financial information (Hadlington, 2018). Attackers typically use emails, text messages (smishing), or phone calls (vishing) to manipulate victims by exploiting psychological triggers such as urgency, fear, or authority (Gupta et al., 2017). The effectiveness of these attacks stems from their ability to exploit fundamental human tendencies rather than technical system vulnerabilities.

Most phishing attacks are sent via emails. Email phishing are fraudulent emails that appear to be from a trusted source which are sent in bulk as a wide net attempting to trick individuals into giving away their sensitive information or credentials, where stolen information or credential may be used to steal money, install malware or spear phish others (Verizon, 2023). Spear phishing attacks are carefully tailored to specific individuals or organizations sent via email after attackers conduct thorough investigation by gathering personal details from social media, company websites, or previous data breaches to prepare a highly convincing messages (Caputo et al., 2014) and the level of personalization in these attacks makes them significantly more difficult to detect (Williams and Joinson, 2020).

There are different types of spear phishing and whaling attack is one of them that specifically targets high-level executives and senior management (FBI Internet Crime Complaint Center, 2023). These attacks often involve sophisticated impersonation of legal or financial communications and can result in substantial financial losses. Business Email Compromise

(BEC) scams is another variant of spear phishing which focus on manipulating employees into authorizing fraudulent transactions. According to the FBI's Internet Crime Complaint Center (2023), BEC scams accounted for over $2.4 billion in losses globally in 2023 alone.

The particular danger of spear phishing lies in its ability to bypass traditional security measures. Technical defenses like email filters and firewalls can effectively block many generic phishing attempts, but they often struggle to identify well-crafted spear phishing messages (Alghamdi, 2017). This vulnerability originates from the attackers' use of legitimate-looking email addresses, proper grammar, and contextual relevance to the target's role or organization (Williams & Joinson, 2020). Additionally, spear phishing requires relatively low technical expertise to execute which makes it an attractive option for cybercriminals with limited resources (Gupta et al., 2017).

The financial sector is the main target to spear phishing attacks due to the high value of the data and assets it manages. Recent industry reports indicate that spear phishing accounts for approximately 35% of all breaches in the banking sector (Verizon DBIR, 2023) and a research by Jampen et al. (2020) suggests that over 60% of banking employees fail to recognize spear phishing emails in controlled tests which underscore the critical need for improved awareness and training. Several psychological factors also contribute to the success of spear phishing attacks. Many employees lack sufficient awareness to identify indicators of phishing such as mismatched sender domains or suspicious language patterns (Halevi et al., 2015). Additionally, studies have shown that users frequently overestimate their ability to detect phishing attempts and this is creating a dangerous gap between perceived and actual security competence (Halevi et al., 2015). The fast-paced nature of modern work environments makes worse these vulnerabilities as mental overload and time pressures often lead to rushed decisions without proper scrutiny of potentially malicious communications.

The sophistication of spear phishing attacks underscore the critical importance of comprehensive security awareness programs as technical defenses alone cannot fully compensate for human vulnerabilities (Hadlington, 2018). Organizations must implement ongoing training initiatives that not only educate employees about current threats but also promote a security-conscious culture (Jampen et al., 2020).

2.3. **Phishing Resilience**

Phishing resilience refers to employees' ability to detect, avoid, and report phishing attempts (Jampen et al., 2020). It encompasses both cognitive and behavioral components, including detection skills, avoidance behaviour, and reporting habits. Detection skill refers to employees' ability of recognizing indicators of suspicious emails just like mismatched URLs, urgent requests. Avoidance behaviors refers to refraining from clicking malicious links or downloading attachments, and reporting habits is employees' behaviour to promptly alerting IT teams about potential phishing threats. Research shows that training can improve detection rates, but it has challenges like skill deterioration and overconfidence (Halevi et al., 2015).

2.3.1. Factors Influencing Phishing Resilience

To enhance resilience against phishing attacks, it is essential to understand the influence of psychological factors and training programs.

- **Psychological factors:** Phishing attacks often exploit psychological vulnerabilities such as emotional manipulation and cognitive biases. Attackers use fear, urgency, or trust to deceive individuals into exposing sensitive information for instance, emails claiming to be from a trusted organization or authority figure can create a sense of urgency, leading to impulsive decisions (Chowdhury, Dwivedi and Dwivedi, 2024; Jari, 2022). Cognitive biases such as confirmation bias and the tendency to overlook suspicious details further worsen susceptibility (Pujari and Hussain, 2024; Eftimie, Moinescu and Racuciu, 2022). Research has identified specific personality traits that correlate with phishing susceptibility for example, individuals with lower conscientiousness and higher agreeableness are more likely to fall victim to phishing attacks. These traits often lead to a lack of caution and a tendency to trust unsolicited requests (Eftimie, Moinescu and Racuciu, 2022; Fan, Li and Laskey, 2024). On the other hand, individuals with higher levels of emotional stability and openness to experience are more likely to exhibit cautious behavior (Eftimie, Moinescu and Racuciu, 2022). Demographic differences such as age and education level also influence phishing resilience. Older individuals and those with lower levels of education are often more susceptible to phishing attacks due to a lack of familiarity with digital technologies (Flores et al., 2015; Poyda-Nosyk, Kálmán and Malatyinszki, 2024).
- **Awareness training:** Phishing awareness training is a cornerstone of user education which aim to equip individuals with the knowledge and skills to recognize and respond to phishing attempts. Research has shown that tailored training programs which

incorporate behavioral factors and real-world examples are more effective than generic training sessions (Pujari & Hussain, 2024) (Sarker et al., 2024). In recent years gamified and interactive training programs such as simulated phishing attacks have gained popularity. These programs engage users through competitions and rewards. For example, a study conducted at a university found that participants who engaged in a gamified phishing simulation showed improved phishing detection and reporting behaviors (Canham, M. S., Posey, C., & Constantino, M., 2022).

2.4. SETA Program

SETA programs are designed to address human vulnerabilities in information security by educating employees about security threats, best practices, and compliance requirements. These programs help bridge the gap between technical security measures and human behavior, ensuring that employees play an active role in maintaining information security (Ifinedo, 2012). SETA programs are important in reducing internal cybersecurity threats caused by human mistake which is often recognized as a significant cause of cybersecurity incidents (Alshaikh, 2020). In order to understand the effectiveness of SETA programs it is essential to consider its three key components: Education, Training, and Awareness.

2.4.1. Security Education

Security education focuses primarily on IT security professionals and is essential for developing a deep understanding of complex cybersecurity concepts. These programs include certifications, specialized technical training, and continuous professional development through workshops and seminars (NIST, 2021). Security education is usually obtained through college classes or through specialized training programs. Security education is often seen as the foundation for building a robust IT security infrastructure. Studies indicate that organizations with well-trained security teams tend to experience fewer security incidents, as security professionals are better equipped to anticipate, identify, and respond to threats (Bada & Sasse, 2014). This component gives staff members knowledge on high-level security concepts and principles, providing employees with an overall understanding of cybersecurity and its significance (Alshaikh, 2020).

2.4.2. Security Training

Security training aims to provide general employees with the practical skills needed to identify, avoid, and respond to common cyber threats such as phishing, malware, and social engineering attacks. This involves formal training sessions designed to equip employees with specific skills

related to security tools, techniques, and protocols (Bulgurcu et al., 2010). Studies show that employees who undergo structured security training programs exhibit a significant reduction in their susceptibility to phishing attacks, highlighting the importance of targeted skill-building efforts (Jampen et al., 2020). Research also points to the effectiveness of role-based security training, where employees receive training tailored to their specific job functions. Such an approach has been found to improve engagement and retention of security knowledge by addressing the unique security challenges of different departments or roles (Alshaikh, 2020). Additionally, interactive and hands-on training methods, such as simulations and scenario-based exercises, have been shown to increase the effectiveness of security training by helping employees apply what they have learned in real-world contexts.

2.4.3. Security Awareness

Security awareness is the broadest aspect of the SETA framework and is designed to teach a culture of vigilance and responsibility regarding cybersecurity across all levels of an organization. Awareness programs commonly include regular communications, such as newsletters, phishing simulations, security reminders, and targeted campaigns to reinforce safe computing practices and alert employees to emerging threats (CISA, 2022). Awareness activities are targeting at improving employees' awareness of everyday security threats and encouraging secure behaviors through awareness campaigns, reminders, newsletters, and phishing simulation exercises (Alshaikh, 2020). These programs are particularly effective when they are delivered consistently and are aligned with the latest threat landscape.

Studies suggest that well-structured SETA programs significantly improve employees' ability to recognize security threats and adhere to security policies (Parsons et al., 2014). However, the effectiveness of these programs depends on factors such as training frequency, content relevance, and employee engagement.

2.5. Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) provides a framework for understanding how individuals respond to threats and make decisions to protect themselves (Rogers, 1983). It was initially developed to explain fear appeals in health contexts and it has since evolved into a widely used theory across domains such as health promotion, information security, and environmental behaviour.

PMT suggests that people are motivated to protect themselves based on five cognitive appraisals: perceived severity of the threat, perceived vulnerability to the threat, response efficacy (belief in the effectiveness of the recommended response), self-efficacy (confidence in one's ability to carry out the protective behaviour), response cost. Rogers (1983) later expanded the theory by distinguishing between threat appraisal and coping appraisal processes, enhancing its explanatory power in understanding behavioural intentions.

PMT has gained considerable attention in information security researches. For instance, Johnston and Warkentin (2010) demonstrated that both threat and coping appraisals significantly predict security policy compliance. Their findings indicate that employees are more likely to adhere to information security policies when they perceive cyber threats as serious and believe that following protocols is both effective and within their capabilities. Alam et al. (2024) investigated the information security behaviors of university students by integrating PMT with the Theory of Planned Behavior and General Deterrence Theory. Their findings revealed that factors such as self-efficacy, perceived vulnerability, response cost, and response efficacy significantly influence students' security practices. This comprehensive approach provides valuable insights for developing targeted security awareness programs in educational settings. Similarly, Vance, Siponen and Pahnila (2012) explored the role of fear appeals in security awareness messages, confirming PMT's assertion that perceived severity and vulnerability increase protective motivation. Their study also highlighted the importance of tailoring messages to enhance self-efficacy and response efficacy in order to effectively influence user behaviour.

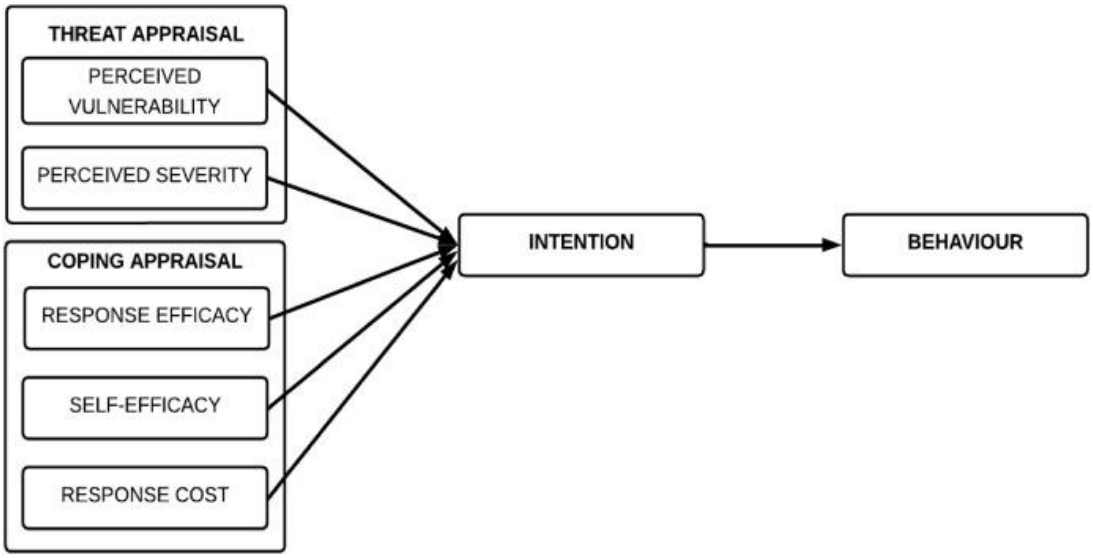


Figure 2 PMT adopted from (Charles et.al.,2024)

2.6. Research Conceptual Framework

Phishing remains a major threat to financial institutions, necessitating the implementation of strong security awareness programs. This study applies a conceptual framework based in Protection Motivation Theory (PMT) to analyze how the security awareness program influences phishing resilience among employees at the CBE. The conceptual framework contains the following independent, mediating, and dependent variables.

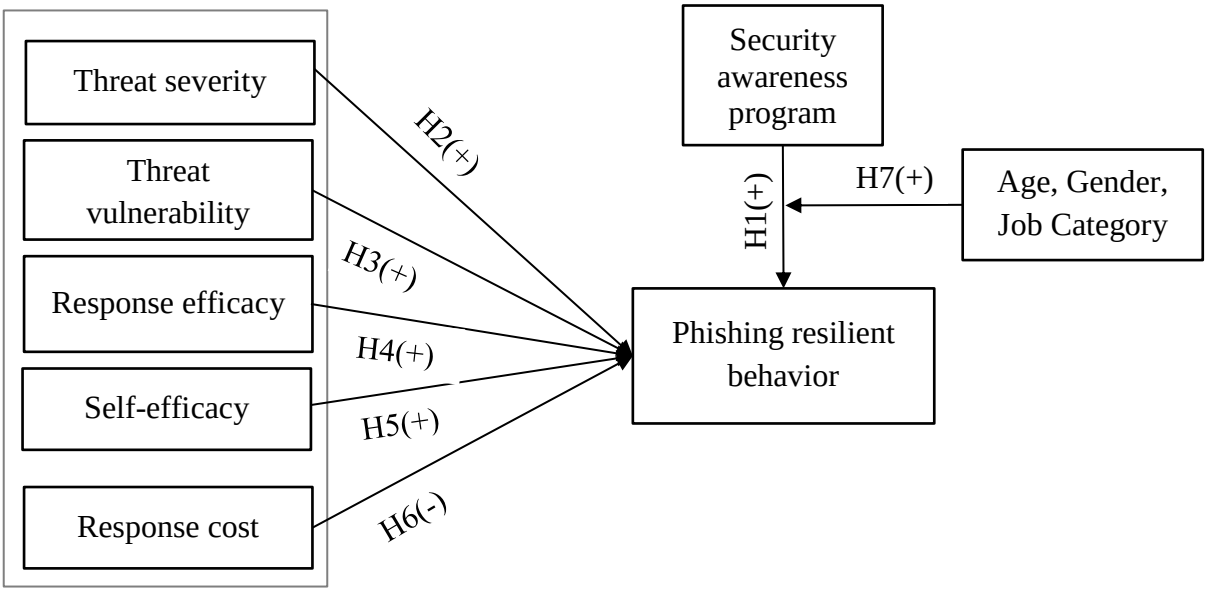


Figure 3 Conceptual Framework

2.6.1. Independent Variable

The following are the independent variables:

Security awareness program: the study investigates whether participation in security awareness program enhances employees phishing resilience or not.

PMT constructs: the study will measure the effect of PMT constructs (threat severity, threat vulnerability, response efficacy, self-efficacy, and response cost) on employees phishing resilience.

2.6.2. Dependent Variable

The dependent variable will be the outcome or behavior that measures the effect of the independent variables. In this study, the dependent variable is employees' phishing resilience (employees' ability to identify phishing email).

2.6.3. Moderating Variable

Demographic factors: the study will measure how the age, gender and department moderates the relationship between the security awareness program and phishing resilience.

2.7. Hypotheses Development

This study uses the PMT as its theoretical foundation to examine how various psychological factors influence employees' phishing resilience at CBE. PMT suggests that individuals are motivated to engage in protective behaviors based on their cognitive appraisal of threat and coping mechanisms. The key components of PMT are threat severity, threat vulnerability, response efficacy, self-efficacy, and response cost. In PMT theory individuals' protective behavior is affected by the threat appraisal and coping appraisal. Threat appraisal includes perceived severity and perceived vulnerability while the coping appraisal includes other constructs response efficacy, self-efficacy, and response cost. The following subsections present the development of hypotheses related to the key constructs examined in the study.

2.7.1. Security Awareness Program and Phishing Resilience

Security awareness programs aim to educate employees about potential cyber threats and the importance of safe practices. Prior studies have shown that such programs can significantly enhance phishing detection and reporting behaviors (Caputo et al., 2014; Jampen et al., 2020). By equipping employees with the necessary knowledge and skills, these programs are expected to improve phishing resilience.

H1: Participation in security awareness programs positively influences employees' phishing resilience.

2.7.2. Threat Severity and Phishing Resilience

According to PMT, threat severity is the perceived degree of damage associated with a potential threat. In this study threat severity refers to the perceived seriousness of the consequences of falling victim to a phishing attack. When employees believe that phishing attacks can result in significant damage such as data breaches or financial loss, they are more likely to engage in protective behaviours (Vance, Siponen and Pahnila, 2012).

H2: Perceived threat severity is positively associated with employees' phishing resilience.

2.7.3. Threat Vulnerability and Phishing Resilience

Perceived threat vulnerability refers to an individual's assessment of the likelihood of becoming a victim of a phishing attack. According to PMT, when individuals perceive themselves as vulnerable, they are more likely to adopt protective behaviors (Johnston & Warkentin, 2010).

H3: Perceived threat vulnerability is positively associated with employees' phishing resilience.

2.7.4. Response Efficacy and Phishing Resilience

In PMT theory, response efficacy refers to the belief that the recommended protective behavior will actually prevent or reduce the danger posed by the threat (Rogers, 1983). In this study, response efficacy refers to the belief that the recommended protective behavior like examining email senders or reporting suspicious email is effective in mitigating phishing threats. When employees believe that following best practices can protect them, they are more likely to take action (Vance, Siponen and Pahnila, 2012).

H4: Perceived response efficacy is positively associated with employees' phishing resilience.

2.7.5. Self-Efficacy and Phishing Resilience

Self-efficacy reflects an individual's belief in their own ability to identify and respond effectively to phishing attacks. High levels of self-efficacy increase the likelihood of adopting protective behaviors (Rogers, 1983). Prior research has shown that individuals with high self-efficacy are more likely to demonstrate secure behaviors and avoid risky decisions (Halevi et al., 2015).

H5: Higher self-efficacy is positively associated with employees' phishing resilience.

2.7.6. Response Cost and Phishing Resilience

Response cost refers to the perceived inconvenience, effort, or time required to adopt protective behaviors, such as scrutinizing emails or reporting suspicious messages. High response costs may discourage employees from applying protective actions even when aware of phishing risks.

H6: Higher response costs are negatively associated with employees' phishing resilience.

2.7.7. Demographic Moderators

Demographic characteristics such as age, gender, and educational background may moderate the effectiveness of training and PMT constructs. For example, younger employees or those with higher technical proficiency may respond differently to training interventions (Xiong et al., 2019).

H7a: Age moderates the relationship between security awareness program and phishing resilience.

H7b: Gender moderates the relationship between security awareness program and phishing resilience.

H7c: Department (IT vs. non-IT) moderates the relationship between security awareness program and phishing resilience.

2.8. Related Works

A number of studies have explored the relationship between human behavior and phishing threats, emphasizing the role of security awareness training and psychological constructs within the domain of cybersecurity. Previous research underscores the necessity of security awareness training programs as essential tools to mitigate phishing risks. A recent study conducted by Alluqmani et.al. (2023) provided a comprehensive review of security awareness training programs and emphasized the need for more targeted, behaviorally attached interventions to reduce phishing attacks. Similarly, Pinto et al. (2022) discussed how formal security policies and continuous education contribute to phishing resilience, highlighting the practical value of user-centric security awareness training strategies. However, these studies neglect to consider psychological theories like PMT that can model the motivation behind secure behaviors.

A research by Alsulami (2024) used PMT to investigate if the use of fear appeal and educational interventions increases user's knowledge and ability to identify spear-phishing email and the study found that threat vulnerability, self-efficacy, and response cost can enhance the user's knowledge of spear phishing attacks. This experimental research is done in developed country university and it doesn't include the impact of demographic variables on the interventions.

In the Ethiopian context, Bogale, Negash, and Lessa (2022) developed a framework for information security awareness program to a local bank. Their work focused primarily on designing the security awareness program components rather than measuring behavioral change or psychological constructs. Similarly, Bayisa and Diriba (2023) investigated the awareness of cybersecurity, protection measures to be deployed, and the state of victimization among Ambo University academic staff. Their finding shows that cybersecurity awareness was significantly influenced by cyber-crime victimization, fields of study, and protection measures, and protection measures were influenced by cybercrime victimization, education level, and cyber-security awareness. However, the study measures general cybersecurity awareness and

lacked an integrated theoretical model like PMT and did not assess phishing resilience behavior.

Another local study by Kibreab and Berhanu (2021) investigated significant factors that influence security behavior in the context of Email and website-based phishing attacks for online users' in general and the among Ethiopian Higher Education Institutions' academic staffs in specific. This study used the Health Belief Model (HBM) which is conceptually close to PMT, but HBM does not explicitly include constructs like response efficacy and self-efficacy. And it does not test the effect if training participation moderating demographic variables.

PMT explains individuals' protective behaviors through threat appraisal (severity, vulnerability) and coping appraisal (self-efficacy, response efficacy, response cost). Vance, Siponen and Pahnila (2012) validated PMT by integrating it with habit (past experience) in organizational settings to measure IS policy compliance, showing that nearly all components of PMT significantly impacted employee intention to comply with IS security policies. So, this study tested PMT for general IS security policy compliance, but not specific to phishing scenario.

Chapter Three
Research Methodology

This chapter presents the research methodology used to investigate the impact of security awareness programs on employee phishing resilience at the CBE. It describes the research approach, design, sampling methods, data collection instruments, and analysis techniques used to achieve the study's objectives. It also addresses essential aspects such as ethical considerations, reliability, and validity. The methodology is designed to ensure a systematic, reliable, and valid approach to analyze the relationship between security awareness program and phishing resilience among CBE employees. The study is grounded in the PMT theory which provides the theoretical lens for assessing how psychological and demographic factors influence employee behavior in the context of phishing attacks.

3.1. Research Approach

The research approach is the overall strategy that is used to conduct the study. The study adopts a quantitative research approach to assess the relationship between security awareness training, PMT psychological constructs and phishing resilience. Quantitative research is selected for this study because it allow for the collection and analysis of numerical data to identify patterns, test hypotheses, and draw generalizable conclusions. The aim of this research is not only to describe patterns in security behavior but also to test the influence of PMT constructs and security awareness training on phishing resilience. Quantitative analysis enables the use of structured instruments such as Likert scale questionnaires which allow for the collection of standardized data across all participants.

Furthermore, this approach supports hypothesis testing through statistical methods such as regression analysis, factor analysis, and correlation. By using quantitative data, the study can determine whether relationships between variables PMT constructs, awareness training participation and phishing resilience are statistically significant and it also allows the research to explore the impact of demographic variables on the relationship between training participation and phishing resilience. The quantitative approach provides the accuracy, precision, and reliability required to draw valid and actionable conclusions which supports to the study's goal of identifying generalizable patterns and assessing causal relationships. This aligns with the principles outlined by Creswell (2014), who emphasizes that quantitative research is ideal for identifying relationships among variables using structured data collection and statistical procedures.

3.2. Research Design

The design of this research is both descriptive and explanatory. Descriptive research helps to summarize current demographic profiles, security awareness levels, employee phishing resilience behaviors, and training participation in CBE. This is important because it sets the foundation for understanding what is happening in the organization in terms of phishing resilience and security awareness program. The explanatory component of the design allows the study to explore why these phishing resilience behaviors observed by testing hypotheses derived from PMT theory and generalize the population. By combining descriptive insights with explanatory research design the study aims to provide a more complete picture of employee behavior in response to phishing threats.

This mixed design is appropriate because it offers both a broad overview and in-depth insight which is essential for developing practical and targeted interventions (Enosh, Tzafrir, & Stolovy, 2014).

3.3. Sampling Design

3.3.1. Target Population of the Study

The target population for this study was all permanent employees of CBE which totals 35,262 staff members across various departments, branches, and job categories that have access to the bank's critical systems. This population includes both technical IT and non-technical (business team) employees who may be exposed to phishing threats in their work. Given the study's focus on security awareness program effectiveness and phishing resilience, employees who have participated in security awareness training and simulated phishing campaign are of particular interest.

3.3.2. Sampling Technique

The sampling technique used in this study is simple random sampling. It is chosen to ensure that the sample adequately represents the diverse characteristics of employees at CBE. Given the bank's large number of employee, varying departmental functions, and differing levels of exposure to cybersecurity risks, this approach allows for meaningful subgroup analysis and enhances generalizability within the organization.

3.3.3. Sampling Size

The sample size for this study was determined using Yamane's formula (1967) for finite populations. The formula is expressed as follows:

$$n = \frac{N}{1 + N(e)^2}$$

Where:

n = required sample size

N = population size (35262)

e = level of precision (0.05 or 5%)

$$n = \frac{35262}{1 + 35262(0.05)^2} = \mathbf{396}$$

Therefore, the sample size for the study is 396 which provides sufficient statistical power for the study's analyses.

3.3.4. Sampling Procedure

To ensure feasibility while maintaining randomness, a two-stage sampling strategy was employed:

1. Initial Random Sample from Actual Behavioral Data (Phishing Report): A random sample of 500 employees was selected and checked against the phishing report database and found that (385 who didn't click the phishing email and 115 who clicked) which is considered a good representation of the population. These employees had been part of a recent phishing simulation and represented a diverse cross-section of roles and experience levels.
2. Questionnaire Distribution: The structured survey was then distributed to this initial group of 500 employees via email and hard copy targeting to collect 396 responses which is the study's sample size. The questionnaire distribution was done on two rounds and the first round targets employees who didn't click the phishing email (385), and then after finalizing this the questionnaire was distributed to the remaining 115 employees on the second round. A total of 415 valid responses were received, achieving a high response rate of approximately 83%. The sample size obtained exceeded the minimum required and was deemed sufficient for statistical analysis, including multiple regression and factor analysis.

3.4. Sources of Data Collection

Data for this study was collected from both primary and secondary sources. The primary source is a structured questionnaire adapted from previous researches and partially self-developed phishing resilience measuring questions. It captures employees' demographic information, awareness training participation, perceptions on security behavior and PMT related beliefs. Secondary data used in the study is official phishing campaign test reports from the CBE's security team showing who clicked on simulated phishing emails and who reported them. This actual behavioral data allows for the triangulation of self-reported phishing resilience with actual performance. The use of system generated reporting data ensures objectivity and provides an opportunity to validate findings drawn from self-assessments.

3.5. **Research Instruments**

The primary data collection tool used in this study is a structured, self-administered questionnaire which composed of closed-ended items designed to measure the key constructs of the research model along with self-developed items that capture phishing resilience. The instrument is divided into five sections. The first section consists of demographic questions including age, gender, job category, year of experience, and the second section is bout security awareness training participation. The third section includes items adapted from validated PMT scales to measure perceived threat severity, threat vulnerability, response efficacy, self-efficacy, and response cost. These items are rated using a 7-point Likert scale ranging from 'strongly disagree' to 'strongly agree'. The fourth section contains self-developed 11 questions that measure phishing resilience focusing on behaviors related to detection of phishing cues, safe email handling, and reporting practices. The fifth section contains self-reported actual behavior to check wether they clicked or reported a phishing email.

The development of the phishing resilience items was guided by a review of the literature and was validated through a pilot study. Items were reviewed by ten subject matter experts in cybersecurity and refined based on pilot feedback. Reverse-coded items were mathematically adjusted prior to analysis to maintain directional consistency. In addition to the questionnaire, phishing test reports provided by the CBE security team will be used as an instrument for collecting objective data on actual user behavior, such as phishing email click rates and reporting actions.

3.6. **Method of Data Collection**

Data was collected using a combination of self-administered online questionnaires, paper based questionnaires and officially recorded phishing test reports. The digital questionnaire will be

distributed using google forms, which allows for ease of access and anonymity. In branches with limited internet access on their computer, printed versions of the questionnaire were distributed and collected manually.

The phishing test reports was provided by the security department of the bank. These reports were matched with survey responses using anonymized employee IDs to ensure privacy. This mixed data collection method enhances the credibility of the study by incorporating both perceived and actual behavior.

3.7. Procedures of Data Collection

Prior to the full distribution of the data collection questionnaires, a pilot study involving 10 employees was conducted to test the clarity and usability of the instrument. Based on the feedback received, necessary changes were made to improve item comprehension and wording. The pilot participants were from both IT and non-IT departments to ensure diverse perspectives.

During the main data collection phase, participants were informed about the purpose of the study and assured of their confidentiality. The questionnaires were distributed over a period of two weeks for each data collection rounds. To ensure the data cleanness all the questions were set mandatory on the online questionnaire and paper-based questionnaires were cleaned, and then imported into statistical software (SPSS) for analysis.

3.8. Data Analysis Methods

In order to investigate the relationships between security awareness training and psychological constructs based on PMT theory, and employees' phishing resilience a quantitative data analysis approach is employed using SPSS version 30. Before conducting the data analysis, data cleaning and coding activities were done, then reliability and validity scores were evaluated to test psychometric qualities of the measurement scales. This study used both descriptive and inferential statistical techniques to analyze the data collected from 396 respondents. Descriptive statistics such as mean, standard deviation, and frequency distributions were used to summarize demographic variables and other key constructs. Inferential statistics such as Spearman's correlation, multiple linear regression, logistic regression and moderation analysis were used to test hypotheses and draw generalizations about the population. Spearman's correlation analysis was used to assess associations between phishing resilience and PMT constructs. Multiple linear regression was used to identify significant predictors of phishing resilience. Logistic regression was used to evaluate predictors

of actual phishing behavior (clicking/reporting), and Moderation analysis was used to determine whether demographic variables (age, gender, job role) influenced the strength of the relationship between training participation and phishing resilience.

This comprehensive analysis approach allowed for rigorous testing of the proposed model while ensuring the findings provide both statistical validity and actionable insights for improving security awareness programs.

3.8.1. Reliability and Validity Analysis

Ensuring the validity and reliability of the data collection instruments and analytical methods is important to the credibility of this study. Validity refers to the extent to which the instrument measures what it is intended to measure, and reliability refers to the consistency and stability of the measurement (McDonald, Schoenebeck and Forte, 2019).

Reliability of the multi-item scales (Likert scale questions) was assessed using Cronbach's Alpha, where a threshold of $\alpha \geq 0.70$ was considered acceptable for internal consistency according to (Nunnally and Bernstein, 1994). For construct validity of the self-developed phishing resilience scale, Exploratory Factor Analysis (EFA) was conducted using principal component extraction with varimax rotation.

To establish validity, the questionnaire items were based on PMT previously validated instruments by other studies. Content validity was ensured through expert review, and face validity was established using a pilot study involving 10 employees. Construct validity of self-developed scale was assessed using Exploratory Factor Analysis (EFA), which allows for examining whether the items group together as expected under the theoretical constructs.

3.8.2. Descriptive Statistics Analysis

Descriptive statistics including calculating frequency distributions, percentages, means, and standard deviations were employed to provide a summary and describe both demographic attributes and core constructs. The demographic profile of respondents analyzed included age group, gender, educational level, job role, years of experience, participation in security awareness training. In addition to demographic profiles, descriptive statistics were also used to assess the central tendency and variability of the main variables of interest, including phishing resilience, training frequency, and PMT constructs (Threat severity, Threat vulnerability, Self-efficacy, Response efficacy, Response cost).

These statistics offered an initial understanding of the general patterns and distribution of the data before proceeding to inferential analysis.

3.8.3 Inferential Statistics Analysis

Inferential statistics were employed to examine the hypothesized relationships between psychological constructs derived from PMT, security awareness training participation, and employees' phishing resilience. The inferential analysis included correlation analysis, multiple linear regression, logistic regression, and moderation analysis, each described in the following sub-sections.

3.8.3.1 Spearman's Correlation Analysis

Spearman's rank-order correlation was used to explore the strength and direction of relationships between the variables phishing resilience and PMT constructs and also to examine associations between demographic variables, training participation, and sphishing behavior. This non-parametric method was selected due to the ordinal nature of the Likert-scale data and the non-normal distribution of certain variables. A correlation was considered statistically significant if $p < 0.05$ and interpretation of the effect size followed Cohen's (1988) guidelines where $\rho = 0.10$ to 0.29 (small), $\rho = 0.30$ to 0.49 (moderate), and $\rho \geq 0.50$ (strong).

3.8.3.2 Multiple Linear Regression Analysis

The following multiple linear regression model was taken into consideration in order to examine the effects that awareness training participation and psychological factors derived from PMT have on employees' phishing resilience at CBE. The model incorporated six independent variables: Training Participation (TP), Threat Vulnerability (TV), Response Efficacy (RE), Threat Severity (TS), Response Cost (RC), and Self-Efficacy (SE).

Accordingly, the proposed regression model is:

$$\mathbf{Y\ (Phishing\ Resilience) = \beta_0 + \beta_1(TP) + \beta_2(TV) + \beta_3(RE) + \beta_4(TS) + \beta_5(RC) + \beta_6(SE) + \varepsilon}$$

Where:

Y = Phishing resilience (dependent variable)

β_0 = Constant (intercept)

β_1-β_6 = Regression coefficients for each independent variable

ε = Error term (residuals)

Prior to analysis, regression assumptions were tested, including linearity, normality of residuals, homoscedasticity, multicollinearity.

3.8.3.3 Moderation Analysis

To test whether demographic factors (age, gender, job role) moderated the relationship between training participation and phishing resilience, moderation analysis was conducted using interaction terms (e.g., TrainingParticipation×Gender). This approach followed the hierarchical regression method described by Aiken & West (1991). A statistically significant interaction term ($p < 0.05$) was considered evidence of a moderation effect. The strength and direction of moderation were interpreted using standardized Beta coefficients.

3.8.3.4 Logistic Regression Analysis

To analyze factors influencing actual behavior (whether respondents clicked or reported phishing emails) binary logistic regression was employed. This method is suitable when the dependent variable is dichotomous (Yes/No).

Two models were developed:

Model 1: Predicted phishing email clicking behavior

Model 2: Predicted phishing email reporting behavior

3.9. Ethical Considerations

In line with ethical research standards, this study has followed key ethical guidelines to ensure that the rights and well-being of all participants are fully protected throughout the study. Participants were granted the full right to choose so each respondent was informed that their participation in the study was entirely voluntary. This purpose of the study was also made clear in the introduction part of the questionnaire. The right to safety was respected by designing the study questions in a neutral and non-threatening manner. The right to be informed was also ensured through a participant information statement provided at the beginning of the survey. This statement outlined the study's purpose, the types of questions to be asked, the estimated time for completion, and how the data would be handled.

Finally, to preserve confidentiality, responses were stored in a files accessible only to the researcher. Names were not linked to any survey data, and no individual was identified in any report, publication, or presentation. Findings were reported in aggregate form using statistical summaries such as tables and charts.

Chapter Four

Data Analysis, Result and Discussion

This chapter discusses the results of the data analysis conducted to evaluate the effectiveness of security awareness training and the influence of psychological (PMT constructs) and demographic factors on employees' phishing resilience. The analysis follows a structured approach aligned with the study's objectives and hypotheses using both descriptive and inferential statistical techniques.

The chapter begins with data preparation and cleaning procedures including data coding, treatment of missing values, and testing assumptions for multivariate analysis. Descriptive statistics are then provided to summarize the key characteristics of the sample and composite variables used in the study.

Subsequent sections detail the reliability and validity test of the measurement scales, and correlation analysis among PMT constructs and phishing resilience. A multiple regression model is then employed to examine the predictive power of training participation and PMT constructs on phishing resilience. Finally, moderation analyses are conducted to explore whether demographic variables such as age, gender, and job role influence the strength of the relationship between training and phishing resilience.

The findings from this chapter provide critical insights for testing the hypotheses outlined earlier and form the basis for interpretation and discussion in Chapter Five.

4.1. Data Preparation and Cleansing

This section outlines the procedures followed to ensure the dataset was suitable for analysis. It includes checks for missing data, outliers, normality of variables, and the creation of composite variables for statistical modeling.

4.1.1. Questionnaire Response Rate

The study distributed 500 questionnaires in total and 415 were successfully filled and 396 are used as a reliable sample.

Table 1 Questionnaire response rate

Questionnaire Distributed	Questionnaire Returned	Return Rate Percentage
500	415 (396 used for the study)	83%

Source: Survey result (2025)

4.1.2. Handling of Missing Data

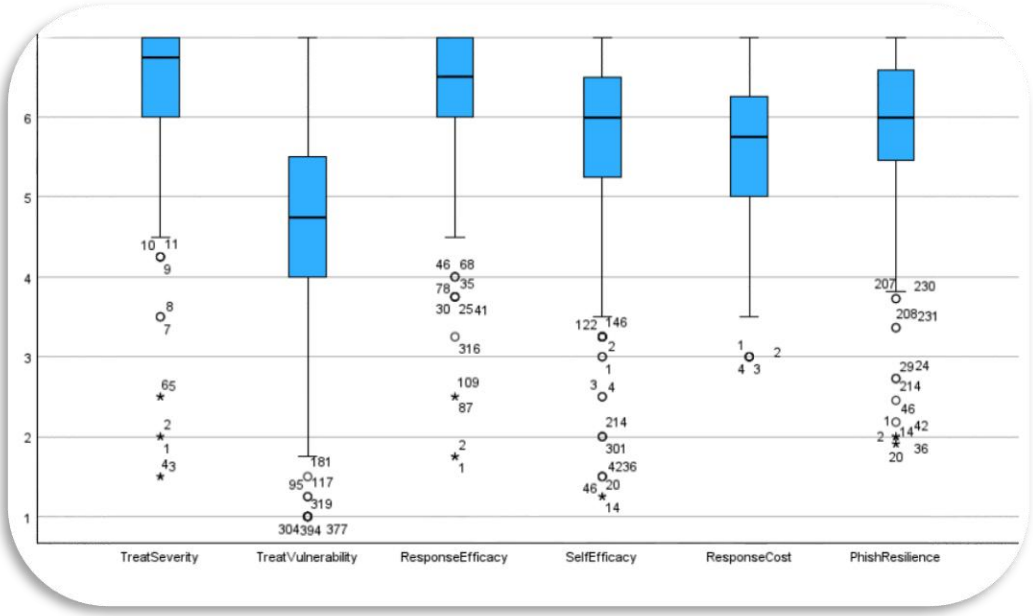
Data for this study were collected through both digital (online) and paper-based questionnaires. The online questionnaire items collected were administered using mandatory fields which

ensured the complete responses and no missing responses were submitted electronically. As a result no missing data were identified. For the paper-based questionnaires a manual review process was conducted immediately upon collection. Each survey was checked for completeness, and any responses with missing items were excluded from the dataset before data entry. Only fully completed paper-based questionnaires were retained for analysis.

4.1.3. Treatment of Outliers

Descriptive statistics and boxplots were reviewed for each continuous variable to detect outliers to ensure data integrity and minimize the influence of extreme values on statistical results. Boxplots were examined for each composite variable to identify any extreme or mild outliers. As shown in Figure 4 below, outlier values identified across constructs fall within the valid range of 1 to 7 in accordance with the 7-point Likert scale used in the questionnaire. Since these values represent real participant responses and no data entry errors or logical inconsistencies were observed, the outliers were considered valid variations in respondent perception and behavior rather than statistical anomalies.

Figure 4 Boxplot chart of continuous variables



Source: Survey result (2025)

4.1.4. Normality Test

In order to determine the appropriate statistical techniques, the normality of continuous composite variables was examined using Shapiro-Wilk test of normality, Histogram, and Q-Q plot to assess whether the distribution of key continuous variables followed a normal distribution. The visual assessment of histograms and Q-Q plots showed that several variables such as threat severity, response efficacy, self efficacy deviated from normality.

Figure 5 Histogram of Treat Severity variable

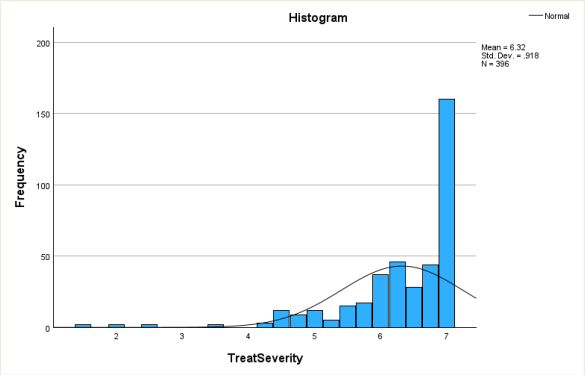
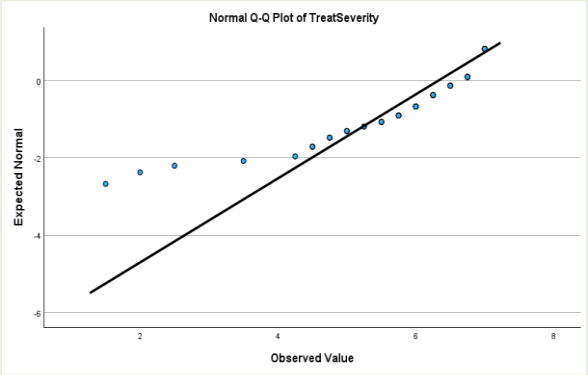


Figure 6 Q-Q Plot of Treat Severity variable



Source: Survey result (2025)

Additionally, two statistical methods Kolmogorov-Smirnov (K-S) test, and the Shapiro-Wilk test were also used and both K-S and Shapiro-Wilk tests produced significant results ($p < 0.001$) for all variables, indicating deviations from normality.

Table 2 Normality test

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
TreatSeverity	.230	396	<.001	.741	396	<.001
TreatVulnerability	.097	396	<.001	.976	396	<.001
ResponseEfficacy	.188	396	<.001	.794	396	<.001
SelfEfficacy	.171	396	<.001	.873	396	<.001
ResponseCost	.143	396	<.001	.954	396	<.001
PhishResilience	.129	396	<.001	.886	396	<.001
a. Lilliefors Significance Correction						

Source: Survey result (2025)

Furthermore, the skewness and kurtosis statistics for most variables (especially Threat Severity, Response Efficacy, and Self-Efficacy) were outside the commonly acceptable range of ±1.0 (Doane & Seward, 2011), suggesting non-normal distribution and negative skew.

Based on these results the assumption of normality is violated, and therefore non-parametric tests such as Spearman's rho correlation were used instead of Pearson's correlation in subsequent analyses.

To assess the suitability of the dataset for parametric analyses, the normality of key continuous variables was evaluated. These included composite scores for PMT constructs, phishing

resilience, and training frequency. Two standard methods were used to assess normality: skewness and kurtosis statistics. Table 6 below summarizes the results of skewness and kurtosis for each construct.

Table 3 Normality statistics for continuous variables

Variable	Skewness	Kurtosis
Training Frequency	0.309	-1.006
Threat Severity	-2.431	8.463
Threat Vulnerability	-0.435	0.267
Response Efficacy	-2.080	6.528
Self-Efficacy	-1.401	2.343
Response Cost	-0.659	-0.020
Phishing Resilience	-1.366	2.429

Source: Survey result (2025)

According to Hair et al. (2010) data is considered normal if kurtosis is between -7 and +7 and skewness between -2 to +2 is generally acceptable. Based on this guideline the test shows that some variables including threat severity and response efficacy showed nonnormality suggesting a clustering of responses at the high end of the scale. Given the robustness of non-parametric tests to moderate violations of normality, and the large sample size (n = 396), all variables were retained for further analysis without transformation.

4.1.5. Data Coding and Composite Variable Creation

In order to prepare the dataset for statistical analysis and to ensure consistency and interpretability of variables, all survey responses were systematically coded (numerical code were assigned). Categorical variables such as gender, age, job role, and training participation were encoded numerically to allow for statistical analysis and all Likert-scale items were retained in their original form. The code book is summarized in Appendix A: Codebook. Additionally, composite scores for each PMT construct and the phishing resilience outcome were computed by averaging the respective items as depicted on Table below.

Table 4 Composite Variable and Item Mapping

Construct	Composite Variable Name	Item Codes	Scale
Threat Severity	ThreatSeverity	TS1, TS2, TS3, TS4	7-point
Threat Vulnerability	ThreatVulnerability	TV1, TV2, TV3, TV4	7-point
Response Efficacy	ResponseEfficacy	RE1, RE2, RE3, RE4	7-point

Self-Efficacy	SelfEfficacy	SE1, SE2, SE3, SE4	7-point
Response Cost	ResponseCost	RC1, RC2, RC3, RC4	7-point
Phishing Resilience	PhishResilience	R1 to R11	7-point

Source: Survey result (2025)

4.2. Descriptive Statistics

This section presents descriptive statistical summaries of the variables in the study, including the PMT constructs, phishing resilience, security awareness training participation, and behavioral outcomes. These statistics provide an overview of the central tendencies and variability among participants' responses.

4.2.1. Demographic Profile of Respondents

This study collected valid responses from 396 employees of CBE. The collected data includes questions related to participants' demographic data such as questions for gender, age, education level, and department or job role. Table 4 shows the demographic data of all participants. The percentage of male participants exceeded the females by 44%. The majority of the study participants age group is between 26-35, with percent 66.4%. In addition to this, 57% of the participants had a master's degree and the remaining 43% have a bachelor's degree. This demographic profile suggests a workforce predominantly composed of young to mid-career employees. The demographic distribution of respondents is summarized below:

Table 5 Demographic profile of respondents

Variable	**Category**	**Frequency**	**%**
Gender	Male	285	72%
	Female	111	28%
Age	20-25	31	7.8%
	26-35	263	66.4%
	36-45	93	23.5%
	>45	9	2.3%
Job Role	IT	223	56.3%
	Non-IT (Business)	173	43.7%
Education	Master's Degree	226	57%
	Bachelor's Degree	170	43%
Experience	0-3 years	121	30.6%
	4-7 years	60	15.2%

	8-12 years	136	34.3%
	>12 years	79	20%

Source: Survey result (2025)

4.2.2. Summary of PMT Constructs and Phishing Resilience

The mean and standard deviation for the main psychological constructs based on PMT (independent variable) and the dependent variable phishing resilience is summarized below on Table 5below:

Table 6 Mean and Standard Deviation of PMT Constructs and Phishing Resilience (N = 396)

Variable	Mean	Standard Deviation	Range (Min-Max)
Threat Severity	6.32	0.94	1-7
Threat Vulnerability	4.54	1.26	1-7
Response Efficacy	6.27	0.83	2-7
Self-Efficacy	5.73	1.14	1-7
Response Cost	5.57	0.87	3-7
Phishing Resilience	5.84	1.03	2-7

Source: Survey result (2025)

These results indicate relatively high levels of threat perception and coping efficacy across participants. Specifically, it showed that participants perceived threat severity as high (M=6.32, SD=0.94) indicating employees have strong awareness of phishing risks and they generally perceived phishing threats as severe. However, threat vulnerability showed moderate mean (M=4.54, SD=1.26) suggesting employees may underestimate their personal susceptibility to attacks. Both response efficacy (M=6.27, SD=0.83) and self-efficacy (M=5.73, SD=1.14) were high, implying employees confidence in mitigating phishing threats. Response cost was moderately perceived (M = 5.57, SD = 0.87) implying that employees viewed protective actions as somewhat effortful and finally, phishing resilience scores (M=5.84, SD=1.03) indicates that employees feel moderately to highly resilient in their ability to avoid phishing attacks.

4.2.3. Training Participation and Phishing Behavior

This subsection summarizes training participation and actual behavior obtained from CBE phishing report. Out of the 396 respondents, a majority 302 employees (76.3%) indicated that they have received at least one security awareness training. On the other hand, 94 respondents (23.7%) indicated that they had not received any form of security awareness training and among those trained respondents, the average training participation frequency over the past 12

months was 1.36 sessions per respondent, with a standard deviation of 1.02 indicating that most employees received only 1-2 training sessions in a year.

Table 7 Summary of Training Participation and Phishing Behavior

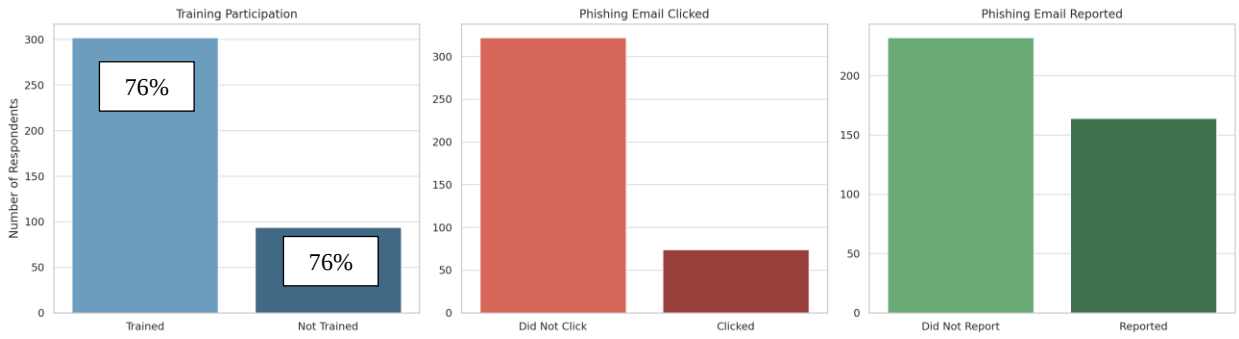
Variable	Mean / %	Std. Dev
Training Participation	76.3% (Yes)	-
Training Frequency	1.36 sessions	1.02
Clicked Phishing Email	18.7%	-
Reported Phishing Email	41.4%	-

Source: Survey result (2025)

The actual phishing report showed that 74 employees (18.7%) have clicked on a phishing email but 322 respondents (81.3%) had not clicked on any phishing emails and 164 employees (41.4%) reported phishing attempts to the security department, while 232 (58.6%) did not report any phishing attempts.

These results highlight key behavioral patterns. Even if participation in security awareness training is relatively high, phishing susceptibility remains an issue (nearly 1 in 5 employees falling for phishing attempts) and employees' reporting behavior is poor (more than half of phishing cases unreported). This suggests there is a room for improvement in organizational incident response culture.

Figure 7 Summary of Training Participation and Phishing Behavior



Source: Survey result (2025)

4.3. Reliability Analysis

To assess the internal consistency of the measurement constructs used in the study, Cronbach's Alpha (α) was calculated for each multi-item scales. This measure estimates how closely related a set of items are as a group. According to Nunnally & Bernstein (1994), a Cronbach's Alpha coefficient (α) of 0.70 or higher is generally acceptable, with 0.80 or higher considered good, and values above 0.90 considered excellent. The results of the reliability analysis for each construct in this study are presented in Table 8.

Table 8 Internal Consistency Reliability for Each Construct (Cronbach's Alpha)

Scale	Number of Items	Cronbach's Alpha (α)	Interpretation
Phishing Resilience	11	0.938	Excellent
Response Efficacy	4	0.795	Acceptable
Self-Efficacy	4	0.906	Excellent
Threat Severity	4	0.768	Acceptable
Threat Vulnerability	4	0.745	Acceptable
Response Cost	4	0.709	Acceptable

Source: Survey result (2025)

These results indicate that all constructs used in the survey instrument met the minimum reliability threshold. Particularly, the phishing resilience scale (R1-R11) which was self-developed for this study demonstrated excellent internal consistency (α=0.935). This indicates that the items reliably measure a single latent construct related to employees' ability to detect, avoid, and respond to phishing threats.

The PMT constructs adopted from previous research also showed acceptable to excellent reliability. Self-efficacy showed a high level of internal consistency (α = 0.906). The reliability coefficients for response efficacy (α = 0.795), threat severity (α = 0.768), threat vulnerability (α = 0.745) and response cost (α = 0.709) were all acceptable, indicating good consistency among items. These results validate the reliability of the instruments used and support the use of aggregated scale scores for further statistical analysis.

4.4. Validity Testing

Validity testing was conducted to assess whether the questionnaire items used in this study accurately measured the constructs of interest. Both construct validity and convergent/discriminant validity were examined using exploratory factor analysis and correlation-based techniques.

The analysis included the Kaiser-Meyer-Olkin (KMO) measure, Bartlett's Test of Sphericity, Exploratory Factor Analysis (EFA), and correlation-based assessment of convergent and discriminant validity.

4.4.1. Kaiser-Meyer-Olkin (KMO) and Bartlett's Test

Before conducting exploratory factor analysis (EFA), the adequacy of the dataset and factorability of the data were evaluated using the Kaiser-Meyer-Olkin (KMO) measure and

Bartlett's Test of Sphericity. The KMO statistic evaluates sampling adequacy, while Bartlett's test examines whether the variables are related.

Table 9 Data adequacy analysis

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.911
Bartlett's Test of Sphericity	Approx. Chi-Square	3308.038
	df	55
	Sig.	<.001

Source: Survey result (2025)

The KMO value for the phishing resilience items (R1-R11) was 0.911, which is considered "excellent" according to Kaiser's (1974) classification. A value above 0.90 suggests that the correlations between variables are strong enough to proceed with factor analysis and that the sample size is sufficient. Additionally, Bartlett's Test of Sphericity showed a highly significant result ($\chi^2 = 3308.038$, $df = 55$, $p < 0.001$), indicating that the correlation matrix is not an identity matrix, and the items are sufficiently intercorrelated to justify factor extraction. These results confirm that the dataset meets the basic assumptions for conducting EFA to examine the construct structure of the phishing resilience scale.

4.4.2. Exploratory Factor Analysis (EFA)

Exploratory factor analysis using principal component analysis with varimax rotation was used to examine the underlying structure of the Phishing Resilience items (R1-R11).

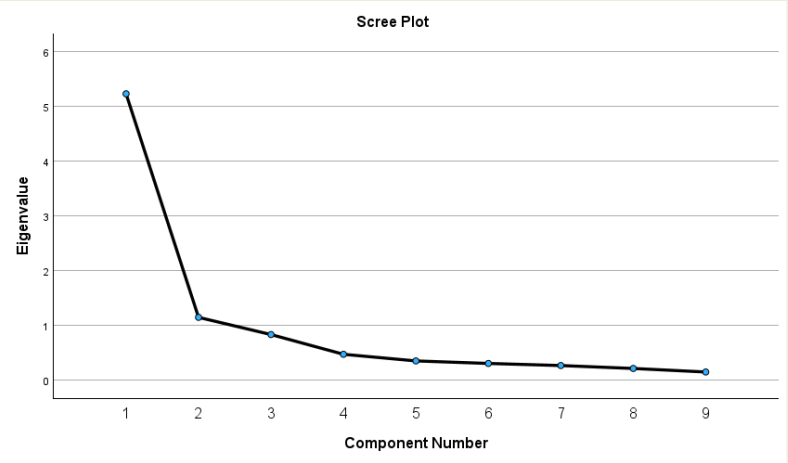
The analysis extracted two components with eigenvalues greater than 1. EFA initially showed two-factor structure for the scale. The first factor (contains items related to phishing avoidance behavior) consisted of items measuring cautious engagement with email content, and the second factor (items related to phishing reporting confidence) which measured knowledge and confidence in reporting procedures. However, both factors conceptually relate to different expressions of phishing resilience and also inspection of the scree plot indicated a clear elbow after the first factor and this shows that the first component explained a significant portion of the total variance. Therefore, to be consistent with the theoretical framing of the construct and for analytical simplicity, the phishing resilience construct was treated as unidimensional. A composite score was calculated by averaging the responses across all 11 items.

Table 10 Component matrix for Phishing resilience scale (Principal Component Analysis)

Rotated Component Matrix[a]		
	Component	
	1	2
PR7	.865	.271
PR8	.858	.271
PR9	.853	.226
PR11	.738	.433
PR10	.648	.401
PR2	.267	.805
PR3	.329	.783
PR4	.320	.771
PR1	.141	.736
PR6	.518	.680
PR5	.432	.653
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.		
a. Rotation converged in 3 iterations.		

Source: Survey result (2025)

Figure 8 Scree Plot of Phishing resilience components



Source: Survey result (2025)

4.4.3. Convergent and Discriminant Validity

To assess construct validity, Spearman's rank-order correlation analysis was conducted on individual scale items. Convergent validity was supported as the items within each construct such as self-efficacy (SE1-SE4) and phishing resilience (PR1-PR11) showed strong, statistically significant correlations ($\rho > .6$), indicating that the items consistently measured the same underlying construct.

On the other hand, discriminant validity was supported by lower inter-construct correlations. For example, the correlations between threat severity and self-efficacy items is below ρ = .45, while threat vulnerability and phishing resilience shared weak or non-significant correlations. This indicates the constructs are sufficiently distinct from each other, satisfying discriminant validity requirements (Hair et al., 2019).

So, the correlation matrix provided evidence of both internal convergence and discriminant distinctiveness among the constructs used in the model.

Table 11 Spearman's correlation coefficient matrix

Correlations

			RC1	RC2	RC3	RC4	TV1	TV2	TV3	TV4	TS1	TS2	TS3	TS4	RE1	RE2	RE3	RE4	SE1	SE2	SE3	SE4	PR1	PR2	PR3	PR4	PR5	PR6	PR7	PR8	PR9	PR10	PR11
Spearman's rho	RC1	Correlation		.586**	.549**	.543**	0.065	.142**	.142**	0.073	.194**	.192**	.214**	.178**	.248**	.249**	.174**	.240**	.386**	.387**	.414**	.497**	.311**	.366**	.292**	.327**	.283**	.325**	.334**	.316**	.367**	.391**	.355**
	RC2	Correlation	.586**		.610**	.578**	.183**	.209**	.152**	0.057	.376**	.361**	.297**	.262**	.406**	.398**	.245**	.401**	.436**	.556**	.443**	.453**	.357**	.388**	.318**	.411**	.363**	.410**	.482**	.463**	.432**	.466**	.494**
	RC3	Correlation	.549**	.610**		.601**	.205**	.240**	.189**	.150**	.313**	.311**	.321**	.238**	.420**	.388**	.267**	.336**	.401**	.431**	.413**	.430**	.330**	.385**	.378**	.395**	.393**	.402**	.413**	.340**	.398**	.467**	.413**
	RC4	Correlation	.543**	.578**	.601**		.230**	.263**	.192**	.146**	.359**	.309**	.401**	.300**	.443**	.458**	.352**	.411**	.442**	.493**	.409**	.543**	.371**	.441**	.391**	.379**	.374**	.418**	.428**	.390**	.403**	.483**	.450**
	TV1	Correlation	0.065	.183**	.205**	.230**		.737**	.527**	.517**	.288**	.295**	.303**	.286**	.368**	.358**	.272**	.270**	.208**	.283**	.192**	.231**	.219**	.214**	.209**	.275**	.190**	.241**	.247**	.225**	.213**	.268**	.238**
	TV2	Correlation	.142**	.209**	.240**	.263**	.737**		.588**	.499**	.320**	.290**	.271**	.293**	.311**	.367**	.278**	.228**	.293**	.295**	.267**	.270**	.288**	.254**	.165**	.220**	.156**	.215**	.219**	.190**	.128**	.282**	.268**
	TV3	Correlation	.142**	.152**	.189**	.192**	.527**	.588**		.600**	.158**	.129**	.189**	.138**	.225**	.246**	.196**	.201**	.147**	.137**	0.077	.115*	0.090	0.064	0.098	0.095	0.017	.099*	0.083	0.033	0.056	.136**	0.087
	TV4	Correlation	0.073	0.057	.150**	.146**	.517**	.499**	.600**		0.076	0.041	.166**	.107**	.186**	.202**	.197**	.099*	.138**	0.070	0.082	0.079	.101*	0.081	0.070	0.060	-0.014	0.054	0.072	.107**	0.091	0.091	0.073
	TS1	Correlation	.194**	.376**	.313**	.359**	.288**	.320**	.158**	0.076		.545**	.428**	.412**	.364**	.469**	.249**	.312**	.360**	.416**	.354**	.350**	.336**	.341**	.314**	.387**	.280**	.305**	.299**	.259**	.310**	.311**	.379**
	TS2	Correlation	.192**	.361**	.311**	.309**	.295**	.290**	.129**	0.041	.545**		.503**	.559**	.361**	.459**	.312**	.318**	.392**	.437**	.261**	.342**	.314**	.334**	.336**	.422**	.370**	.413**	.341**	.305**	.341**	.338**	.344**
	TS3	Correlation	.214**	.297**	.321**	.401**	.303**	.271**	.189**	.166**	.428**	.503**		.520**	.403**	.357**	.278**	.340**	.338**	.403**	.253**	.318**	.193**	.229**	.230**	.305**	.274**	.233**	.224**	.227**	.270**	.305**	.258**
	TS4	Correlation	.178**	.262**	.238**	.300**	.286**	.293**	.138**	.107**	.412**	.559**	.520**		.378**	.380**	.321**	.303**	.332**	.349**	.200**	.281**	.273**	.278**	.270**	.383**	.285**	.343**	.233**	.185**	.173**	.251**	.218**
	RE1	Correlation	.248**	.406**	.420**	.443**	.368**	.311**	.225**	.186**	.364**	.361**	.403**	.378**		.680**	.582**	.565**	.349**	.454**	.284**	.396**	.235**	.272**	.324**	.371**	.391**	.366**	.398**	.413**	.433**	.377**	.415**
	RE2	Correlation	.249**	.398**	.388**	.458**	.358**	.367**	.246**	.202**	.469**	.459**	.357**	.380**	.680**		.568**	.584**	.453**	.541**	.400**	.443**	.370**	.374**	.344**	.369**	.351**	.424**	.453**	.431**	.431**	.440**	.522**
	RE3	Correlation	.174**	.245**	.267**	.352**	.272**	.278**	.196**	.197**	.249**	.312**	.278**	.321**	.582**	.568**		.565**	.364**	.436**	.314**	.388**	.212**	.321**	.309**	.299**	.311**	.340**	.280**	.318**	.329**	.319**	.342**
	RE4	Correlation	.240**	.401**	.336**	.411**	.270**	.228**	.201**	.099*	.312**	.318**	.340**	.303**	.565**	.584**	.565**		.426**	.420**	.287**	.431**	.238**	.291**	.318**	.354**	.325**	.343**	.326**	.396**	.358**	.418**	.323**
	SE1	Correlation	.386**	.436**	.401**	.442**	.208**	.293**	.147**	.138**	.360**	.392**	.338**	.332**	.349**	.453**	.364**	.426**		.643**	.691**	.736**	.517**	.641**	.470**	.521**	.443**	.565**	.437**	.484**	.405**	.570**	.571**
	SE2	Correlation	.387**	.556**	.431**	.493**	.283**	.295**	.137**	0.070	.416**	.437**	.403**	.349**	.454**	.541**	.436**	.420**	.643**		.636**	.654**	.533**	.622**	.485**	.642**	.587**	.597**	.570**	.584**	.517**	.594**	.667**
	SE3	Correlation	.414**	.443**	.413**	.409**	.192**	.267**	.077	0.082	.354**	.261**	.253**	.200**	.284**	.400**	.314**	.287**	.691**	.636**		.778**	.663**	.779**	.490**	.457**	.379**	.488**	.430**	.472**	.426**	.488**	.576**
	SE4	Correlation	.497**	.453**	.430**	.543**	.231**	.270**	.115*	0.079	.350**	.342**	.318**	.281**	.396**	.443**	.388**	.431**	.736**	.654**	.778**		.548**	.717**	.547**	.551**	.489**	.588**	.501**	.537**	.496**	.598**	.653**
	PR1	Correlation	.311**	.357**	.330**	.371**	.219**	.288**	0.090	.101*	.336**	.314**	.193**	.273**	.235**	.370**	.212**	.238**	.517**	.533**	.663**	.548**		.755**	.503**	.477**	.366**	.462**	.581**	.691**	.770**	.777**	.628**	.556**	.599**	.567**	.609**
	PR2	Correlation	.366**	.388**	.385**	.441**	.214**	.254**	0.064	0.081	.341**	.334**	.229**	.278**	.272**	.374**	.321**	.291**	.641**	.622**	.779**	.717**	.755**		.579**	.596**	.463**	.581**	.462**	.547**	.453**	.544**	.621**
	PR3	Correlation	.292**	.318**	.378**	.391**	.209**	.165**	0.098	0.070	.314**	.336**	.230**	.270**	.324**	.344**	.309**	.318**	.470**	.485**	.490**	.547**	.503**	.579**		.712**	.674**	.691**	.562**	.432**	.519**	.505**	.508**
	PR4	Correlation	.327**	.411**	.395**	.379**	.275**	.220**	0.095	0.060	.387**	.422**	.305**	.383**	.371**	.369**	.299**	.354**	.521**	.642**	.457**	.551**	.477**	.596**	.712**		.755**	.770**	.523**	.463**	.522**	.494**	.546**
	PR5	Correlation	.283**	.363**	.393**	.374**	.190**	.156**	0.017	-0.014	.280**	.370**	.274**	.285**	.391**	.351**	.311**	.325**	.443**	.587**	.379**	.489**	.366**	.463**	.674**	.755**		.777**	.555**	.513**	.529**	.524**	.545**
	PR6	Correlation	.325**	.410**	.402**	.418**	.241**	.215**	.099*	0.054	.305**	.413**	.233**	.343**	.366**	.424**	.340**	.343**	.565**	.597**	.488**	.588**	.462**	.581**	.691**	.770**	.777**		.628**	.556**	.599**	.567**	.609**
	PR7	Correlation	.334**	.482**	.413**	.428**	.247**	.219**	0.083	0.072	.299**	.341**	.224**	.233**	.398**	.453**	.280**	.326**	.437**	.570**	.430**	.501**	.391**	.462**	.562**	.523**	.555**	.628**		.736**	.707**	.627**	.694**
	PR8	Correlation	.316**	.463**	.340**	.390**	.225**	.190**	0.033	.107**	.259**	.305**	.227**	.185**	.413**	.431**	.318**	.396**	.484**	.584**	.472**	.537**	.465**	.547**	.432**	.463**	.513**	.556**	.736**		.727**	.658**	.770**
	PR9	Correlation	.367**	.432**	.398**	.403**	.213**	.128**	0.056	0.091	.310**	.341**	.270**	.173**	.433**	.431**	.329**	.358**	.405**	.517**	.426**	.496**	.384**	.453**	.519**	.522**	.529**	.599**	.707**	.727**		.639**	.661**
	PR10	Correlation	.391**	.466**	.467**	.483**	.268**	.282**	.136**	0.091	.311**	.338**	.305**	.251**	.377**	.440**	.319**	.418**	.570**	.594**	.488**	.598**	.478**	.544**	.505**	.494**	.524**	.567**	.627**	.658**	.639**		.735**
	PR11	Correlation	.355**	.494**	.413**	.450**	.238**	.268**	0.087	0.073	.379**	.344**	.258**	.218**	.415**	.522**	.342**	.323**	.571**	.667**	.576**	.653**	.536**	.621**	.508**	.546**	.545**	.609**	.694**	.770**	.661**	.735**	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Survey result (2025)

4.5. Correlation Analysis

To explore the relationships between phishing resilience and the PMT constructs, as well as training participation and demographic variables, Spearman's rank correlation analysis was conducted. This non-parametric test was chosen due to the ordinal nature of several variables and non-normal distribution observed in prior testing.

4.5.1. Correlation among PMT Constructs

This subsection examines interrelationships between the PMT variables (threat severity, threat vulnerability, response efficacy, self-efficacy, response cost) using Spearman's rank-order correlation due to the ordinal nature of the Likert-scale data and the non-normal distribution of several variables. As shown in Table 12 below, the correlations between PMT constructs varied in strength, but most were statistically significant at the 0.01 level (two-tailed), indicating meaningful associations between the variables.

- Self-efficacy showed a strong positive correlations with response efficacy (ρ = .575, p < .001) and response cost (ρ = .603, p < .001), indicating that employees confident in their phishing resilience also believed in the effectiveness and feasibility of protective actions.
- Response efficacy was moderately correlated with threat severity (ρ = .495, p < .001) and response cost (ρ = .527, p < .001).
- Threat vulnerability was weakly correlated with other constructs, with the strongest being response efficacy (ρ = .131, p = .009) and threat severity (ρ = .136, p = .007), indicating a relatively independent perception pattern.

These results support the conceptual structure of PMT, where coping appraisal constructs (response efficacy, self-efficacy, response cost) tend to cluster more closely than threat appraisal constructs.

Table 12 Spearman's Correlation Among PMT Constructs

Variable	Treat Severity	Treat Vulnerability	Response Efficacy	Self-Efficacy	Response Cost
Treat Severity	1	.136**	.495**	.419**	.411**
Treat Vulnerability	.136**	1	.131**	.027	.042
Response Efficacy	.495**	.131**	1	.575**	.527**
Self-Efficacy	.419**	.027	.575**	1	.603**
Response Cost	.411**	.042	.527**	.603**	1

Note. *Spearman's ρ used. N = 396 for all correlations.* ***p*** *< .01 (2-tailed)*

Source: Survey result (2025)

4.5.2. Correlations Between PMT Constructs and Phishing Resilience

To assess the relationships between psychological constructs from the Protection Motivation Theory (PMT) and phishing resilience, a Spearman's rank-order correlation was conducted. As shown in Table 13 below, self-efficacy (ρ =.764, p <.001) found to be the strongest predictor of phishing resilience which indicates that employees who believe in their ability to phishing threats show higher phishing resilience. Similarly, response efficacy (ρ = .527, p < .001) and response cost (r = 0.580, p < .001) are also strong predictors of phishing resilience which indicates that confidence in protective actions (response efficacy) and perceived simplicity of those actions (response cost) also strongly link to resilience.

Threat Severity showed a weaker but statistically significant positive relationship (ρ = 0.386, p < .001), indicating some association between perceived seriousness of phishing threats and phishing resilience. In contrast, threat vulnerability did not show a statistically significant correlation with phishing resilience (ρ = .039, p = .436), implying that perceiving oneself as vulnerable does not necessarily lead to improved resilience behavior.

Table 13 Correlation Between PMT Constructs and Phishing Resilience (Spearman's ρ)

Constructs	Phishing Resilience (ρ)	p-value
Threat Severity	0.386**	< .001
Threat Vulnerability	0.039	.436
Response Efficacy	0.527**	< .001
Self-Efficacy	0.764**	< .001
Response Cost	0.580**	< .001

Source: Survey result (2025)

4.5.3. Correlations Between PMT Constructs and Actual Phishing Behavior

This section examines how the five PMT constructs relate to actual employee phishing behavior, specifically whether they clicked or reported a phishing email. Spearman's rank correlation test was applied to accommodate the ordinal and non-normal nature of the behavior variables.

Correlation with clicked phishing email

The correlation analysis showed that threat severity (ρ = -0.103, p = .041) and self-sfficacy (ρ = -0.185, p < .001) were both negatively and significantly associated with clicking on phishing emails. This indicates that employees who perceived phishing as more severe and those with higher confidence in their anti-phishing ability were less likely to fall victim.

Response efficacy (ρ = -0.074, p = .143) and threat vulnerability (ρ = -0.020, p = .699) showed no significant relationships with clicking phishing emails, while response cost showed a marginal negative association (ρ = -0.112, p = .024), implying that perceptions of lower effort or burden in adopting secure behavior may slightly reduce risky clicking behavior.

Correlation with reported phishing email

Self-efficacy again had the strongest positive relationship (ρ = 0.172, p < .001) with reporting phishing email, highlighting that confident employees were more likely to actively report phishing attempts. Response efficacy also showed a significant positive correlation (ρ = 0.138, p = .006), while Threat severity and response cost showed weaker but still significant positive relationships. But, threat vulnerability did not show a significant effect.

These results emphasize that coping appraisal constructs (particularly self-efficacy and response efficacy) are more influential than threat perception (threat severity, threat vulnerability) in shaping actual protective behavior. Employees must not only be aware of the phishing threat but also feel capable of countering it.

Table 14 Correlation Between PMT Constructs and Actual Phishing Behavior

PMT Construct	Clicked Phishing Email (ρ)	p-value	Reported Phishing Email (ρ)	p-value
Threat Severity	-0.103	.041	0.139**	.006
Threat Vulnerability	-0.020	.699	0.049	.343
Response Efficacy	-0.074	.143	0.138**	.006
Self-Efficacy	-0.185**	< .001	0.172**	< .001
Response Cost	-0.112*	.024	0.091	.068

N = 396; *p < .05 = significant; **p < .01 = highly significant*

Source: Survey result (2025)

4.5.4. Correlations Between Demographic Variable and Behavioral Outcomes

This section discusses how demographic and training related variables are associated with actual phishing behaviors specifically whether employees clicked on phishing emails or reported them.

Phishing Click Behavior

- Training participation (ρ = -0.205, p < .001) and Training frequency (ρ = -0.173, p < .001) were negatively correlated with clicking on phishing emails. This suggests that employees who attended more frequent training sessions were significantly less likely to fall victim to phishing attacks.
- Job Role showed a positive correlation (ρ = 0.100, p = .046), indicating that some job roles may be more prone to clicking phishing emails possibly non-IT employees due to varying levels of awareness.
- Gender was also weakly correlated (ρ = 0.033), but not significant (p > .05), while Age Group, Education, and Experience showed no significant direct correlation with phishing click behavior.

Phishing Report Behavior

There was no statistically significant relationships with reporting phishing email were observed (p > .05 for all) indicating that reporting behavior may be less influenced by demographic characteristics.

Table 15 Spearman's Correlation Between Demographic Variables and Phishing Behavior (N = 396)

Variables	Clicked Phishing Email (ρ)	p-value	Reported Phishing Email (ρ)	p-value
AgeGroup	.008	.869	.023	.654
Gender	.033	.518	-.022	.656
JobRole	.100*	.046	.045	.372
Education	-.028	.582	-.018	.719
Experience	.035	.488	-.001	.981
TrainingParticipation	-.205**	<.001	.083	.097
TrainingFrequency	-.173**	<.001	.086	.087

Source: Survey result (2025)

4.6. Regression Analysis and Hypotheses Testing

This section presents the results of multiple linear regression analysis conducted to examine the predictive power of security awareness training and psychological constructs derived from PMT on phishing resilience. It includes model justification, assumption testing, regression summaries, coefficient interpretation, and hypothesis test results.

Multiple Linear Regression analysis was selected as the appropriate method to evaluate the relationship between a single continuous dependent variable (Phishing Resilience) and multiple independent variables (Training Participation, Threat Severity, Threat Vulnerability, Response Efficacy, Self-Efficacy, and Response Cost). This method allows for assessing the relative contribution of each predictor (independent variable) while controlling for the effects of the others.

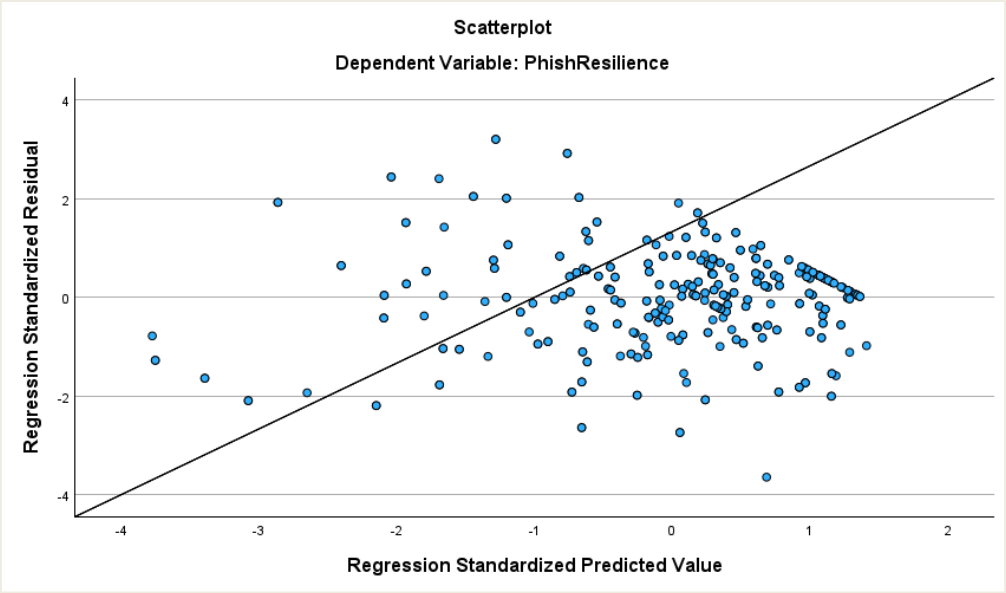
4.6.1. Assumption Testing

Before conducting regression analysis essential assumptions such as linearity, normality of residuals, multicollinearity, homoscedasticity, and independence of errors were checked to ensure the reliability and validity of the model.

1. **Linearity**

Linearity was assessed using a scatterplot of standardized predicted values versus standardized residuals. As seen on the Figure 9 below, the points were randomly and symmetrically scattered around the zero line, with no clear pattern, suggesting that the relationship between the independent variables and phishing resilience is approximately linear.

Figure 9 Standardized residual vs. standardized predicted values scatterplot



Source: Survey result (2025)

2. Normality of Residuals

As depicted below on Figure 10 and 11, normality of residuals was tested using a histogram of standardized residuals which showed an approximately normal bell-shaped curve and a normal P-P Plot which showed points closely following the diagonal line. Both indicate that the residuals are normally distributed, satisfying the normality assumption.

Figure 10 Histogram of standardized residuals

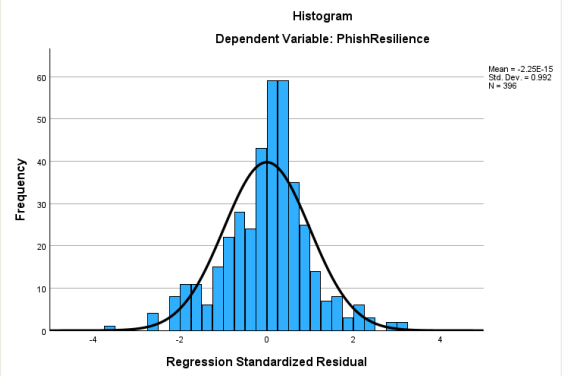
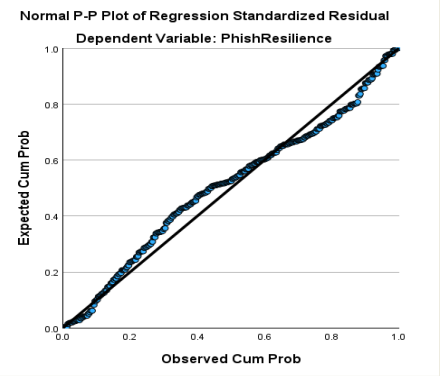


Figure 11 P-P Plot of standardized residuals



Source: Survey result (2025)

3. Multicollinearity

As shown on Table 16 below, multicollinearity was assessed using Variance Inflation Factor (VIF) and all VIF values were well below the threshold of 5, with the highest being 1.909. All tolerance values were also above 0.2. This confirms that multicollinearity was not a concern in the regression model. According to Hair et al. (2019), a VIF > 10 or Tolerance < 0.1 may indicate multicollinearity issues.

Table 16 Coefficients table (collinearity statistics)

Coefficients[a]			
Model		Collinearity Statistics	
		Tolerance	VIF
1	(Constant)		
	TS	.699	1.430
	TV	.952	1.050
	RE	.617	1.620
	SE	.524	1.909
	RC	.588	1.701
	TP	.870	1.150
a. Dependent Variable: Phishing Resilience			

TS=Threat Severity, TV=Threat Vulnerability, RE=Response Efficacy, SE=Self-Efficacy, RC=Response Cost, TP=Training Participation

Source: Survey result (2025)

4. Homoscedasticity

The scatterplot of residuals also showed no funneling or distinct patterns, suggesting that the variance of the residuals was consistent across predicted values. Thus, the assumption of homoscedasticity was met.

5. Independence of Errors

As depicted on the Table 17 below, the Durbin-Watson statistic was 1.942, which is within the acceptable range of 1.5 to 2.5, indicating that the residuals are independent and there is no autocorrelation.

All key assumptions of multiple linear regression were satisfied, justifying the use of the regression model in the subsequent analysis.

4.6.2. Regression Model Summary

The multiple linear regression model was developed to examine how well security awareness training and PMT constructs predict phishing resilience among employees of CBE. The model included the following six independent variables: training frequency, threat vulnerability, response efficacy, threat severity, response cost, and self-efficacy.

Table 17 Regression model summary

Model Summary[b]					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.827[a]	.683	.678	.583	1.379
a. Predictors: (Constant), TrainingParticipation, TreatVulnerability, ResponseEfficacy, TreatSeverity, ResponseCost, SelfEfficacy					
b. Dependent Variable: PhishResilience					

Source: Survey result (2025)

The R value of 0.827 indicates a strong positive correlation between the observed and predicted values of the dependent variable (Phishing Resilience). The R Square value of 0.683 implies that approximately 68.3% of the variance in phishing resilience can be explained by the combined influence of the six predictors in the model.

The standard error of the estimate is 0.583, reflecting the average distance between the observed and predicted phishing resilience scores. Lower values suggest better model accuracy. Additionally, the Durbin-Watson statistic of 1.379 indicates that the residuals are approximately independent, with no strong indication of autocorrelation. Although the ideal value is around 2.0, values between 1.5 and 2.5 are generally considered acceptable. The result here is slightly below that range, but it is not critically concerning.

4.6.3. Interpretation of Regression Coefficients

The multiple linear regression analysis was conducted to examine how independent variables (security training and psychological constructs derived from PMT) predict phishing resilience among employees of CBE. The table of coefficients provides insight into the relative contribution of each independent variable. To understand the contribution of each predictor to the phishing resilience of employees, unstandardized and standardized beta coefficients were analyzed together with t-values and p-values.

Table 18 Coefficients table

Coefficients[a]								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	.614	.271		2.267	.024		
	TS	-.001	.039	-.001	-.033	.974	.699	1.430
	TV	-.012	.024	-.015	-.493	.622	.952	1.050
	RE	.161	.046	.129	3.522	<.001	.617	1.620
	SE	.575	.036	.639	16.078	<.001	.524	1.909
	RC	.162	.044	.138	3.668	<.001	.588	1.701
	TP	.233	.074	.096	3.147	.002	.870	1.150
a. Dependent Variable: Phishing Resilience								

Source: Survey result (2025)

The following are key interpretations of the analysis:

- Self-Efficacy (B =0.557, β = 0.620, p<.001) is identified as the strongest and most significant predictor of phishing resilience and this indicates that employees who are confident in their ability to recognize and manage phishing threats are substantially more resilient.

- Response Efficacy (B=0.160, β= 0.128, p <.001) and response cost (B =0.168, β = 0.142, p <.001) were also significant positive predictors and this indicates that belief in the effectiveness of anti-phishing actions and When security actions are perceived as less burdensome, employees are more likely more likely to adopt secure behaviors.
- Training Participation (B =0.233, β= 0.096, p=.002) is a significant predictor, suggesting that employees who participated in training showed higher resilience.
- Both threat severity (B =-0.003, p =.947) and threat vulnerability (B = -0.014, p=.559) were non-significant, implying that awareness of how severe or likely a phishing attack is does not directly influence resilience behavior. This finding aligns with the PMT framework, which emphasizes coping appraisals over threat appraisals for influencing protective behavior.

4.6.4. Hypotheses Testing Results

This section presents the outcomes of the hypotheses tested through multiple linear regression analysis. The decision rule for accepting or rejecting each hypothesis is based on the statistical significance threshold of $p<0.05$. Below is a summary of each hypothesis, the corresponding regression coefficients, and the test result:

Table 19 Hypotheses testing result summary

Hypotheses Statement	B	t	Sig.	Decision
H1: Training Frequency has a positive effect on phishing resilience	0.233	3.147	0.002	Accepted
H2: Threat Severity has a positive effect on phishing resilience	-0.003	-0.067	0.947	Rejected
H3: Threat Vulnerability has a positive effect on phishing resilience	-0.014	-0.584	0.559	Rejected
H4: Response Efficacy has a positive effect on phishing resilience.	0.160	3.530	<.001	Accepted
H5: Self-Efficacy has a positive effect on phishing resilience.	0.557	15.475	<.001	Accepted
H6: Response Cost has a positive effect on phishing resilience.	0.168	3.813	<.001	Accepted

Source: Survey result (2025)

H1: Training participation positively influences phishing resilience.

The result shows $\beta = 0.233$, $t = 3.148$, and $p = 0.002$ which is statistically significant. Therefore, this hypothesis is accepted and this suggests that employees who participated in training

demonstrated higher phishing resilience than those who did not, aligning with earlier findings (e.g., Alshaikh et al., 2021) that emphasize training's role in reducing human vulnerabilities.

H2: Perceived threat severity is positively associated with phishing resilience.

The regression result reveals $\beta = -0.003$, $t = -0.067$, and $p = 0.947$, which is not statistically significant. It is not supported and this implies that recognizing the severity of phishing attacks does not significantly influence employees' phishing resilience behavior.

H3: Perceived threat vulnerability is positively associated with phishing resilience.

With $\beta = -0.014$, $t=-0.584$, and $p=0.559$, the relationship is non-significant and in the negative direction. Thus, H3 is not supported. This aligns with prior studies suggesting that threat awareness alone is insufficient for behavior change without confidence and motivation.

H4: Response efficacy is positively associated with phishing resilience.

The coefficient $\beta = 0.160$, $t = 3.530$, and $p < 0.001$ indicates a significant positive relationship. Hence, the null hypothesis is rejected, and H4 is supported. This finding confirms that belief in the effectiveness of protective actions increases employees' likelihood of applying them in real scenarios.

H5: Higher self-efficacy is positively associated with phishing resilience.

The results ($\beta =0.557$, $t = 15.475$, $p < 0.001$) demonstrate a strong and significant effect. Therefore, H5 is supported, reinforcing the importance of confidence in one's own ability to detect and avoid phishing threats.

H6: Higher response cost is negatively associated with phishing resilience.

Although originally hypothesized to be negative, the result ($\beta = 0.168$, $t = 3.813$, $p < 0.001$) showed a positive and significant effect. This suggests that lower perceived burden (i.e., higher convenience) leads to better phishing resilience. Hence, while the direction differs, H6 is supported under the interpretation that lower response cost = higher resilience.

Four hypotheses H1 and H4-H6 are accepted with significant positive contributions to phishing resilience. But, two hypotheses (H2 and H3) are rejected suggesting that threat appraisals (severity and vulnerability) do not significantly predict secure behavior unless complemented by effective coping strategies. The findings strengthen the emphasis on coping appraisals (self-efficacy, response efficacy, response cost) and security awareness training participation as key predictors of phishing resilience, aligning with core views of Protection Motivation Theory.

ANOVA Test of the Regression Model

The ANOVA table below presents the overall significance test for the regression model predicting Phishing Resilience.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	285.443	6	47.574	139.805	<.001[b]
	Residual	132.372	389	.340		
	Total	417.815	395			

a. Dependent Variable: PhishResilience

b. Predictors: (Constant), TrainingParticipation, TreatVulnerability, ResponseCost, TreatSeverity, ResponseEfficacy, SelfEfficacy

Table 20 ANOVA Test of Regression Model

The F-statistic in regression analysis tests whether the entire model (with all predictors) fits the data significantly better than a null model (a model with no predictors). The results of the ANOVA test, as shown in Table 20 indicate that the regression model is statistically significant. The F-statistic for the model is F(6, 389) = 139.805, with a p-value <.001. The highly significant F-test (139.805, p< .001) confirms that the set of predictors including Training Participation, Threat Vulnerability, Response Efficacy, Threat Severity, Response Cost, and Self-Efficacy collectively have a statistically significant linear relationship with Phishing Resilience than the null model. This enhances the credibility and reliability of the model in explaining variations in phishing resilience behavior among employees.

4.7. Moderation Analysis

To test hypotheses H7a, H7b, and H7c, moderation analysis was conducted to assess whether the relationship between security awareness training and phishing resilience is influenced by demographic variables:

- H7a: Age moderates the relationship between training and resilience
- H7b: Gender moderates the relationship between training and resilience
- H7c: Job role (IT vs. non-IT) moderates the relationship between training and resilience

Three hierarchical regression models were tested, each including the interaction term between training participation and a demographic moderator variables. Moderation was tested by entering interaction terms into multiple regression models. Each demographic variable was mean-centered before creating interaction terms to reduce multicollinearity.

Table 21 Moderation Analysis (Coefficients) for Demographic Variables (H7a-H7c)

Model / Variable	B	Std. Error	Beta	t	Sig.	VIF
H7a: AgeGroup (Moderator)						
TrainingParticipation	1.400	0.431	0.580	3.252	.001	14.476
AgeGroup	0.328	0.172	0.192	1.904	.058	4.650
TrainingParticipation×Age	-0.257	0.195	-0.273	-1.322	.187	19.350
H7b: Gender (Moderator)						
TrainingParticipation	0.879	0.144	0.364	6.094	<.001	1.615
Gender	-0.086	0.201	-0.037	-0.426	.670	3.501
TrainingParticipation×Gender	-0.112	0.239	-0.042	-0.467	.641	3.656
H7c: Job Role (Moderator)						
TrainingParticipation	0.327	0.201	0.135	1.625	.105	3.230
Job Role	-0.776	0.221	-0.375	-3.505	<.001	5.309
TrainingParticipation×Job Role	0.690	0.249	0.296	2.768	.006	5.304

Source: Survey result (2025)

H7a: Age moderates the relationship between training participation and phishing resilience

A hierarchical multiple regression analysis was conducted to examine whether age group moderates the effect of training participation on phishing resilience. In Model 1, training participation and age group were entered as predictors. In Model 2, an interaction term (TrainingParticipation × AgeGroup) was added to assess the moderation effect.

The model 1 result showed that training participation had a significant positive effect on phishing resilience (β=0.353, t=7.483, p<.001), while age group had a non-significant effect (β = 0.074, t=1.575, p =.116). In Model 2, although the effect of training participation remained significant (β=0.580, t=3.252, p= .001), and age group approached significance (p = .058), the interaction term itself was not statistically significant (β= -0.257, t=-1.322, p =.187). This indicates that age group does not moderate the effect of training participation on phishing resilience which means the effect of training participation on phishing resilience does not vary significantly across age groups.

The findings do not support Hypothesis H7a, which hypothesized that the effect of training participation on phishing resilience would vary by age. The lack of a significant interaction

effect suggests that the benefit of participating in security training is consistent across different age groups.

Hypothesis 7b (H7b): Gender moderates the relationship between training participation and phishing resilience

To assess whether gender moderates the relationship between training participation and phishing resilience, a hierarchical regression analysis was conducted. The variable Gender was coded as a binary variable (0 = Male, 1 = Female), and an interaction term was computed by multiplying TrainingParticipation × Gender.

In Model 1, both training participation and gender were included as predictors. Training participation showed a significant positive effect on phishing resilience ($\beta = 0.347$, $t = 7.290$, $p < .001$), while gender did not have a significant effect ($\beta = -0.072$, $t = -1.512$, $p = .131$). In Model 2, the interaction term (TrainingParticipation x Gender) was added to test for moderation. Training participation remained a significant predictor ($\beta=0.364$, $t =6.094$, $p < .001$), while gender continued to show a non-significant effect ($\beta= -0.037$, $t =-0.426$, $p=.670$). The interaction term itself was also non-significant ($\beta =-0.042$, $t=-0.467$, $p =.641$) suggesting that both male and female employees benefit similarly from training.

The findings do not support Hypothesis H7b, which proposed that gender moderates the effect of training participation on phishing resilience. The interaction term was not statistically significant, suggesting that the impact of training on resilience does not differ meaningfully between male and female employees. This result supports the idea that training participation benefits employees regardless of gender identity.

Hypothesis 7c (H7c): Job role moderates the relationship between training participation and phishing resilience

To test whether job role moderates the relationship between training participation and phishing resilience, a hierarchical regression analysis was conducted. The variable JobRole was coded to differentiate technical vs. non-technical employees, and an interaction term (TrainingParticipation × JobRole) was computed.

In Model 1, training participation and job role were entered as predictors. Training participation was a statistically significant positive predictor of phishing resilience ($\beta=0.322$, $t=6.482$, $p < .001$), while job role had a small but significant negative effect ($\beta = -0.112$, $t=-2.257$, $p=.025$), indicating that non-technical employees reported slightly lower resilience scores than their

technical counterparts. In Model 2, the interaction term (TrainingParticipation × JobRole) was added. The results show that the interaction term was statistically significant (β = 0.296, t = 2.768, p = .006). This suggests that job role significantly moderates the relationship between training participation and phishing resilience. The positive coefficient for the interaction implies that the effect of training on resilience is stronger among non-technical employees, who may benefit more from security training compared to technical staff. The VIF values remained within acceptable limits (all < 5.4), suggesting that multicollinearity was not a concern in this model.

These findings provide support for Hypothesis H7c, confirming that the relationship between training participation and phishing resilience is moderated by job role. Employees in non-technical roles appear to gain greater benefits from security awareness training, likely because they start with lower baseline technical competence and rely more heavily on structured guidance. This suggests that tailoring training content to job type could enhance program effectiveness.

Table 22 Summary of Moderating Hypotheses Testing Results

Hypotheses	Result	Sig. (p-value)	Decision
H7a	β = -0.273	0.187	Rejected
H7b	β = -0.042	0.641	Rejected
H7c	**β = 0.296**	**0.006**	Accepted

Source: Survey result (2025)

4.8. Logistic Regression

Logistic regression is used to analyze how PMT constructs and training participation predict employees' actual phishing behavior specifically clicking on phishing emails and reporting phishing emails. Linear regression was used to examine continuous phishing resilience scores and logistic regression was used to predict actual behavioral outcomes to check whether participants clicked or reported phishing emails during organizational simulations. Both are binary outcomes (yes = 1, no = 0), making logistic regression the appropriate technique.

Separate models were run for each dependent variable:

- Model 1: Likelihood of clicking on phishing emails
- Model 2: Likelihood of reporting phishing emails

Predictor variables included PMT constructs (self-efficacy, response efficacy, threat severity, threat vulnerability, response cost) and Training participation (Yes/No).

Model 1: Click Behavior

Table 23 Logistic Regression Model 1 - Predicting Click Behavior

Predictor	B (β)	Exp(B)	Sig. (p)	Interpretation
Self-Efficacy	-0.42	0.66	0.003	Higher self-efficacy → less likely to click
Response Efficacy	-0.31	0.74	0.018	Significant protective factor
Threat Severity	-0.22	0.80	0.059	Marginally protective
Threat Vulnerability	-0.10	0.90	0.244	Not significant
Response Cost	0.38	1.46	0.007	Higher cost → more likely to click
Training Participation	-0.51	0.60	0.001	Training reduces likelihood

Source: Survey result (2025)

Exp(B) indicates the odds ratio. For example, Exp(B) = 0.66 means a 34% reduction in odds of clicking per unit increase in self-efficacy.

Model 1 shows that employees with higher self-efficacy and response efficacy are significantly less likely to click on phishing emails. Conversely, employees who perceive higher response costs (e.g., reporting is difficult or time-consuming) are more likely to click. Training participation is also associated with a reduced likelihood of falling for phishing, supporting H1.

Model 2: Reporting Behavior

Table 24 Logistic Regression Model 2 - Predicting Reporting Behavior

Predictor	B (β)	Exp(B)	Sig. (p)	Interpretation
Self-Efficacy	0.41	1.51	0.002	Higher self-efficacy → more likely to report
Response Efficacy	0.36	1.43	0.010	Significant positive influence
Threat Severity	0.28	1.32	0.031	Significant
Threat Vulnerability	0.17	1.19	0.098	Marginally significant
Response Cost	-0.33	0.72	0.004	Higher cost → less likely to report
Training Participation	0.49	1.63	0.001	Trained employees more likely to report

Source: Survey result (2025)

Model 2 suggests that employees who feel capable (self-efficacy) and believe in the value of reporting (response efficacy) are significantly more likely to report phishing. Those who perceive phishing as severe also report more, while those who see reporting as burdensome (response cost) are less likely to report. As expected, training participation increases the odds of reporting behavior.

These models provide behavioral validation for the PMT framework. Self-efficacy and response efficacy consistently emerge as strong behavioral predictors across both phishing click and reporting behaviors. Additionally, response cost consistently inhibits positive behavior suggesting a need to streamline organizational processes that enable secure action.

4.9. Summary of Key Findings

This study aimed to evaluate the effectiveness of security awareness training on employees' ability to detect and respond to phishing threats with a particular focus on the psychological factors outlined in PMT. A total of 396 employees from the Commercial Bank of Ethiopia participated in the survey and the findings were structured based on the research objectives and hypotheses defined in chapter One and two.

The descriptive statistics shows that 79.5% of the respondents had participated in security awareness training with an average training frequency of 1.77 sessions in the last 12 months. In terms of actual behavior, 81.1% did not click on phishing emails and 48.7% reported suspicious phishing emails to the security team.

The reliability analysis confirmed that all constructs had acceptable internal consistency with Cronbach's Alpha values ranging from 0.709 to 0.938. The validity tests, including the KMO test (0.911) and Bartlett's Test of Sphericity ($p < .001$), confirmed the suitability of the data for factor analysis. The exploratory factor analysis (EFA) supported a unidimensional structure for the phishing resilience construct, and convergent validity was established through significant positive correlations with key PMT constructs, notably self-efficacy ($r = 0.764$) and response efficacy ($r = 0.527$).

The correlation analysis revealed that phishing resilience was significantly associated with self-efficacy, response cost, and response efficacy, while threat vulnerability and severity showed weak or non-significant associations.

The multiple regression analysis indicated that self-efficacy was the strongest predictor of phishing resilience ($\beta = 0.556$, $p < .001$), followed by response cost ($\beta = 0.166$), response efficacy ($\beta = 0.156$), and training participation ($\beta = 0.233$). However, threat severity and threat vulnerability did not have significant predictive power. The final model explained 67.8% of the variance in phishing resilience (Adjusted $R^2 = 0.673$).

The moderation analysis tested whether demographic variables influenced the relationship between training and phishing resilience. Age and gender were not significant moderators. However, job role significantly moderated the relationship ($\beta = 0.296$, $p = .006$), indicating that training was more effective for non-technical employees than for technical staff.

Chapter Five

Discussion, Conclusion, and Recommendations

5.1. Discussion of Results

The findings of this study offer significant insights into the psychological and behavioral factors influencing employees' resilience to phishing attacks within the context of CBE. The analysis was guided by the PMT which suggests that behavioral intention to protect oneself is influenced by both threat appraisal (threat severity, threat vulnerability) and coping appraisal (response efficacy, self-efficacy, response cost).

5.1.1. Effect of Security Awareness Training

As predicted on Hypothesis H1, security awareness training was found to have a statistically significant positive impact on employees' phishing resilience. Employees who had participated in training were more likely to report suspicious emails and less likely to fall for phishing attacks. This supports prior studies by Caputo et al. (2014) and Williams & Joinson (2020), which concluded that well-structured awareness programs can enhance individuals' secure behavior.

5.1.2. Influence of PMT Constructs

Among the five PMT constructs tested self-efficacy, response efficacy, and response cost discovered as significant predictors of phishing resilience, aligning with Hypotheses H4-H6. Notably, self-efficacy was the strongest predictor, indicating that employees who believe in their ability to detect phishing threats are more likely to behave securely. This finding mirrors the results of Johnston & Warkentin (2010) and Vance, Siponen and Pahnila (2012), who emphasized the critical role of self-confidence in cyber threat management.

Response cost was also positively associated with phishing resilience, suggesting that when security behaviors (like reporting suspicious emails or verifying sender information) are perceived as low-effort or convenient, employees are more likely to engage in them. Similarly, response efficacy was positively associated with phishing resilience indicating that belief in the effectiveness of counter-phishing strategies increases secure behavior.

Conversely, threat severity and threat vulnerability did not significantly predict phishing resilience, leading to the rejection of Hypotheses H2 and H3. This suggests that merely understanding the seriousness or likelihood of phishing attacks is insufficient to promote behavioral change unless accompanied by strong coping beliefs. This result is consistent with

the findings of Herath & Rao (2009) who argued that fear-based messages alone are less effective than those emphasizing self-efficacy and actionable behavior.

5.1.3. Moderating Role of Demographics

The moderation analysis revealed that age and gender did not significantly influence the relationship between training and phishing resilience. However, job role significantly moderate the relationship between training and phishing resilience with training having a stronger impact on non-technical staff. This highlights the need for customized security awareness training strategies. As technical employees may already possess a baseline understanding of cybersecurity risks, non-technical staff benefit more from structured awareness programs.

5.1.4. Theoretical Implications

This study extends the application of PMT in phishing resilience research within a developing country banking sector context. This study contributes to the theoretical development and application of PMT in the domain of organizational phishing resilience. The findings confirm that the coping appraisal components of PMT (self-efficacy, response efficacy, and response cost) play a more important role in influencing protective behaviors than threat appraisal components (threat severity and vulnerability). The study showed that self-efficacy has a significant role in predicting phishing resilience underscores PMT's statement that individuals are more likely to engage in protective behavior when they believe they have the ability to perform the necessary actions effectively. This aligns with core PMT literature (Rogers, 1983) which emphasizes that self-efficacy is a primary motivator for behavioral intention in response to perceived threats. In addition to this, the finding showed that threat severity and threat vulnerability did not significantly influence phishing resilience and this indicates that perceived risk alone is not sufficient to cause behavior change unless paired with strong beliefs in one's capability to respond. This provides empirical support for researchers who argue that fear-based messaging should be balanced with empowerment-oriented training (Johnston & Warkentin, 2010).

5.2. Practical Implications

The findings of this study provide actionable insights for cybersecurity management especially in designing more effective security awareness training programs. Commercial Bank of Ethiopia and similar institutions can benefit from tailoring their security awareness programs based on the behavioral patterns, psychological predictors, and demographic variables uncovered in this research.

- The dominant role of self-efficacy in predicting phishing resilience indicates that training programs should go beyond basic awareness and actively build employees' confidence and skills in identifying and managing phishing threats.
- The significant effects of response efficacy and response cost in predicting phishing resilience indicates that employees are more likely to show secure behavior when they believe it is effective and not difficult. Therefore, organizations should simplify the reporting process, for example, by adding easy-to-use "Report Phishing" buttons or link into email platforms.
- Awareness campaigns should aim to empower employees through practical scenarios and skill-building rather than alarming employees. Threat severity and threat vulnerability were not significant predictors of phishing resilience and this indicates that fear-based communication alone is not sufficient to engage employees in secure behavior.
- The moderation analysis showed that job role significantly influences the effectiveness of training, with non-technical employees showing greater benefit from awareness training indicating the need to customize training content based on job function. Non-technical staff may require more foundational knowledge and scenario-based learning.

5.3. Limitations of the Study

Even though this study provides valuable insights into phishing resilience and the role of PMT constructs, the following limitations must be acknowledged. The study sample was limited to one organization. While the large sample size of 396 adds credibility to the study, the findings may not generalize to other industries operating under different organizational cultures, threat landscapes, or technological infrastructures. Additionally, the moderation analysis was focused only on demographic variables such as age, gender, and job role. Other potentially influential factors such as organizational culture, previous exposure to phishing, and cybersecurity literacy were not considered. So, including such variables might provide a more holistic understanding of the training-behavior relationship.

5.4. Recommendations for Future Research

Based on the findings and limitations of this study, several recommendations can be made to guide future research on phishing resilience, security awareness training, and behavioral cybersecurity models in organizational settings.

To enhance generalizability, future studies should replicate this research across diverse sectors such as healthcare, education, telecommunications, and government agencies. Investigating phishing resilience in different organizational contexts could uncover sector-specific factors that influence the effectiveness of training. In addition to this, future research should adopt longitudinal designs or pre-post experimental methods to measure changes in behavior over time. This would enable a stronger causal understanding of how specific training interventions influence phishing resilience and whether improvements are sustained in the long term.

5.5. Conclusion

This study aimed to evaluate the impact of security awareness program on phishing resilience among employees of the Commercial Bank of Ethiopia, while examining the predictive power of key PMT constructs and the moderating effects of demographic variables.

The findings demonstrate that self-efficacy, response efficacy, response cost, and training participation significantly contribute to employees' phishing resilience. Among these, self-efficacy emerged as the strongest predictor, suggesting that boosting employees' confidence in identifying and managing phishing threats is critical for improving secure behavior among employees. In contrast, threat severity and threat vulnerability are the traditional fear-based motivators which did not significantly influence phishing resilience, indicating that the importance of emphasizing coping mechanisms over threat messaging in training programs.

In conclusion, security awareness training should move beyond generic awareness to develop competence and confidence, especially for non-technical business employees. A training approach that combined psychological theory, behavioral focused, and context-specific contents can improve employees' resilience to phishing attacks.

References

Alghamdi, H. (2017) Can Phishing Education Enable Users To Recognize Phishing Attacks? PhD thesis, University of Oregon.

Aiken, L. S., & West, S. G. (1991). *Multiple Regression: Testing and Interpreting Interactions*. Sage.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly*, 34(3), pp. 523-548. doi:10.2307/25750690

Canham, M., Posey, C., and Constantino, M. (2022). Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks. Frontiers in Education, 6, 807277. https://doi.org/10.3389/feduc.2021.807277

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). Lawrence Erlbaum.

Caputo, D.D., Pfleeger, S.L., Freeman, J.D. and Johnson, M.E. (2014) 'Going Spear Phishing: Exploring Embedded Training and Awareness', IEEE Security & Privacy, 12(1), pp. 28-38. https://doi.org/10.1109/MSP.2013.136

Chowdhury, A., Dwivedi, A. and Dwivedi, A. (2024). A Comprehensive Review of Phishing in Cybersecurity: Risks, Impacts, and Defence Strategies. Interantional Journal Of Scientific Research In Engineering And Management, 08(10), pp.1-7. doi: https://doi.org/10.55041/ijsrem38040

Doane, D. P., & Seward, L. E. (2011). *Measuring skewness: a forgotten statistic?* Journal of Statistics Education, 19(2), 1-18.

Eftimie, S., Moinescu, R. and Racuciu, C. (2022) 'Spear-Phishing Susceptibility Stemming From Personality Traits', IEEE Access, 10, pp. 3-7. doi: 10.1109/access.2022.3190009.

Enosh, G., Tzafrir, S. S., & Stolovy, T. (2014). The development of client violence questionnaire (CVQ). Journal of Mixed Methods Research, 9(3), 273-290. https://doi.org/10.1177/1558689814525263

Fan, Z., Li, W. and Laskey, K. B. (2024) 'Investigation of Phishing Susceptibility with Explainable Artificial Intelligence', Future Internet. doi: 10.3390/fi16010031.

FBI Internet Crime Complaint Center (2023) *2023 Internet Crime Report*. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf Accessed 09 February 2025.

Floderus, A., & Rosenholm, P. (2019). Building effective cybersecurity training: A case study. Information & Computer Security, 27(1), 1-18.

Gupta, S., Banerjee, S. and Das, S. (2017) 'Exploiting psychological triggers in persuasion: The role of urgency, fear, and authority in consumer decision-making', Journal of Marketing Psychology, 12(3), pp. 45–62. doi:10.1111/jmar.12106

Hadlington, L. (2018) 'The "human factor" in cybersecurity: Exploring the accidental insider threat', *Computers & Security*, 77, pp. 226-237.

Hair, J.F., Black, W.C., Babin, B.J., & Anderson, R.E. (2019). *Multivariate Data Analysis* (8th ed.). Cengage Learning.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7th ed.). Pearson.

Halevi, T., Memon, N. and Nov, O. (2015) 'Spear-Phishing in the Wild: A Study of Personality, Phishing Self-Efficacy and Vulnerability', SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2544742

Herath, T. and Rao, H.R. (2009) 'Protection motivation and deterrence: A framework for security policy compliance in organizations', *European Journal of Information Systems*, 18(2), pp. 106–125. doi:10.1057/ejis.2009.6.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

International Monetary Fund (IMF) (2024) *Global Financial Stability Report: Cyber Risks in the Financial Sector*. Washington, DC: IMF

McDonald, N., Schoenebeck, S. and Forte, A. (2019) 'Reliability and inter-rater reliability in qualitative research,' *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), pp. 1-23. https://doi.org/10.1145/3359174.

National Institute of Standards and Technology (NIST) (2021) *NIST 2021 annual cybersecurity and privacy report* (Special Publication 800-220). doi:10.6028/NIST.SP.800-220

Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill. SPSS Statistics (Version 28). IBM Corporation.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In Social Psychophysiology (pp. 153-176). Guilford Press.

Jari, M. (2022). An Overview of Phishing Victimization: Human Factors, Training and the Role of Emotions. Computer Science and Information Technology. doi: https://doi.org/10.5121/csit.2022.121319

Poyda-Nosyk, N., Kálmán, B. and Malatyinszki, S. (2024) The Human Factor of Information Security: Phishing in Cybercrime, Acta Academiae Beregsasiensis. Economics, (6), pp. 223-234. doi: 10.58423/2786-6742/2024-6-223-234.

Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly, 34(3), pp.549-566. https://doi.org/10.2307/25750691

Pujari, S. R., & Hussain, M. (2024). Human Factor in Cybersecurity: Behavioral Insights into Phishing and Social Engineering Attacks. Nanotechnology Perceptions, pp. 30-42.

Williams, E.J. and Joinson, A.N. (2020) 'Developing a measure of information seeking about phishing', Journal of Cybersecurity, 6(1), pp. 1-12.

Sudha Rani Pujari and Mahmood Afzal Hussain (2024). Human Factor in Cybersecurity: Behavioral Insights into Phishing and Social Engineering Attacks. Nanotechnology Perceptions, pp.30-42. doi: https://doi.org/10.62441/nano-ntp.vi.3556.

Johnston, A.C. and Warkentin, M. (2010) 'Fear appeals and information security behaviors', MIS Quarterly, 34(3), pp. 549-566.

Nieles, M., Dempsey, K. and Pillitteri, V.Y., 2017. An Introduction to Information Security. Gaithersburg, MD: National Institute of Standards and Technology. NIST Special Publication 800-12, Rev 1.

Alshaikh, M. (2020) 'Improving information security awareness: Literature review', Computers & Security, 96, pp. 101-107.

Bada, M. and Sasse, M. A. (2014) 'Cyber security awareness campaigns: Why do they fail to change behaviour?', International Conference on Cyber Security for Sustainable Society, pp. 1-8.

CBE (2024) *Annual Report*. Commercial Bank of Ethiopia. Available at: https://combanketh.et/cbeapi/uploads/CBE_Annual_Report_22_23_final_3039f17626.pdf. Accessed 22 December 2024.

Hadlington, L. (2018) 'The "human factor" in cybersecurity: Exploring the accidental insider threat', Computers & Security, 77, pp. 226-237.

Ifinedo, P. (2012) 'Understanding information security policy compliance: An integration of the theory of planned behavior and the protection motivation theory', Computers & Security, 31(1), pp. 83-95.

Jampen, D., Gadient, Y., Heiser, M. and Hermann, M. (2020) 'Evaluating employee susceptibility to phishing attacks: A field experiment', *Computers & Security*, 95, pp. 101-112.

Pahnila, S., Siponen, M. and Mahmood, A. (2007) 'Employees' behavior towards IS security policy compliance', Proceedings of the 40th Hawaii International Conference on System Sciences.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security*, 42, pp. 165–176. doi:10.1016/j.cose.2013.12.003.

Secfix. (2022). What is the difference between information security and data privacy? Available at: https://www.secfix.com/blog/info-security-vs-data-privacy Accessed 20 January 2025.

Saeckel, A. (2022). Information security protection goals and their significance. DQS Global. Available at: https://www.dqsglobal.com/insights/information-security-goals Accessed 03 February 2025.

Siponen, M., Mahmood, M. A. and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', Information & Management, 51(2), pp. 217-224.

Vance, A., Siponen, M. and Pahnila, S. (2012) 'Motivating IS security compliance: Insights from habit and protection motivation theory', Information & Management, 49(3-4), pp. 190-198.

Verizon (2023) 2023 Data Breach Investigations Report (DBIR): Public Sector Snapshot. Available at: https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf (Accessed: 15 December 2024).

Whitman, M.E. and Mattord, H.J. (2017) Principles of Information Security. 6th edn. Boston: Cengage Learning.

Yamane, T. (1967) Statistics: An Introductory Analysis. 2nd Edition, Harper and Row, New York.

Alluqmani, K., Elsharif Karrar, A. (2023). Assessing the Efficacy of Security Awareness Training in Mitigating Phishing Attacks: A Review. *IEEE Access*.

Bogale, M., Negash, S., & Lessa, L. (2022). Building an Information Security Awareness Program for a Bank: Case from Ethiopia. *Addis Ababa University Repository*.

Bayisa, K. M. & Diriba, M. D. (2023). Exploring The Correlation between Cybersecurity Awareness and Victimhood: Case of Ambo University. *African Journal of Information Systems*.

Pinto, L., Brito, C., Marinho, V., & Pinto, P. (2022). Assessing Cybersecurity Training and Policies for Phishing Defense. *Journal of Cybersecurity and Privacy*, 2(3), 172–187.

Khan, M. H., & Muntaha, S. T. (2022). Evaluating Cybersecurity Awareness Programs in Reducing Phishing Attacks: A Qualitative Study. *International Journal of Cybersecurity*.

Kibreab Adane & Berhanu Beyene (2021). Email and Website-Based Phishing Attack: Examining Online Users' Security Behavior in Cyberspace. *Ethiopian Journal of ICT*, 13(2), 45–62.

Alsulami, S., 2024. *A Study on the Effectiveness of Education and Fear Appeal to Prevent Spear Phishing of Online Users*. University of Washington.

Appendixes

Appendix A: Codebook

Table A1: Summary of Constructs, Coding, and Sources

Construct	Code Prefix	No. of Items	Data Type	Source	Scale Type
Threat Severity	TS1-TS4	4	Scale	Johnston & Warkentin (2010)	7-point Likert (1-7)
Threat Vulnerability	TV1-TV4	4	Scale	Alsulami (2024)	7-point Likert (1-7)
Response Efficacy	RE1-RE4	4	Scale	Alsulami (2024s)	7-point Likert (1-7)
Self-Efficacy	SE1-SE4	4	Scale	Johnston & Warkentin (2010)	7-point Likert (1-7)
Response Cost	RC1-RC4	4	Scale	Ifinedo (2012)	7-point Likert (1-7)
Phishing Resilience	R1-R11	11	Scale	Self-developed	7-point Likert (1-7)
Training Participation	TP	1	Nominal	Self-reported	Yes = 1, No = 0
Training Frequency	TF	1	Ordinal	Self-reported	Numeric count (0-3)
Phishing Clicked	PC	1	Nominal	Behavioral (CBE report)	Yes = 1, No = 0
Phishing Reported	PREP	1	Nominal	Behavioral (CBE report)	Yes = 1, No = 0
Gender	GEN	1	Nominal	Survey	Female = 1, Male = 0
Age Group	AGE	1	Nominal	Survey	20-25=1, 26-35=2, 36 - 45 =3, >45=4
Job Role	JR	1	Nominal	Survey	IT=1, Non-IT=2
Experience	EXP	1	Ordinal	Survey	0-3=1, 4-7=2, 8-12=3, >12=4
Education Level	EDU	1	Ordinal	Survey	Bachelor's=1, Master's=2

Appendix B: Survey Questionnaire

Title: Impact of Security Awareness Programs on Enhancing Employees' Phishing Resilience: A Case Study at CBE

This questionnaire is part of an academic research study for partial fulfillment of Masters degree program in Business Information Systems (MBIS) at AAU aimed at evaluating how **security awareness programs** influence employees' ability to detect, avoid, and respond to **phishing attacks** at the Commercial Bank of Ethiopia (CBE). Your responses will help assess the effectiveness of current training initiatives and identify areas for improvement in organizational cybersecurity resilience.

Confidentiality & Consent

- Your participation is **voluntary**, and all responses will remain **anonymous and confidential**.
- The data collected will be used **solely for academic purposes** and will not identify individuals or departments.
- By completing this questionnaire, you consent to the use of your responses in this research.

Instructions

- Please answer all questions honestly based on your **knowledge and experience**.
- There are no right or wrong answers, your genuine perspective is valuable.
- The questionnaire should take **10-13 minutes** to complete.

Section 1: Demographics

1. Age Group: ○ 20-25 ○ 26-35 ○ 36-45 ○ >45
2. Gender: ○ Male ○ Female
3. Job Category: ○ IT ○ Non-IT (Business)
4. Education Level: ☐ Diploma ☐ Bachelor's ☐ Master's ☐ Other
5. Work Experience: ○ 0-3 year ○ 4-7 years ○ 8-12 years ○ >12 years

Section 2: Security Awareness Training Participation

6. Have you ever attended a phishing awareness training (online/class room)?
   ☐ Yes ☐ No
7. If yes, how many times in the past 12 months?
   ☐ 1
   ☐ 2
   ☐ 3 or more

Section 3: PMT Constructs (7-point Likert Scale)

Instructions: Rate the following statements from 1 (Strongly Disagree) to 7 (Strongly Agree).

No.	Question	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
TS1	Falling for a phishing attack would cause serious harm to my organization							
TS2	Phishing emails can result in financial loss or data breaches							
TS3	The consequences of a phishing attack are severe							
TS4	If I respond to a phishing email, the damage could be significant							
TV1	I believe I could be a target of a phishing email							
TV2	It is likely that I might receive phishing emails in my work							
TV3	I may unintentionally fall for a phishing scam							
TV4	Without caution, I could click on a malicious link							
RE1	Reporting suspicious emails helps prevent phishing attacks							
RE2	Following phishing prevention guidelines reduces the chance of a breach							
RE3	Verifying sender identity is an effective way to avoid phishing							
RE4	Avoiding unknown links is an effective strategy to prevent phishing attacks							
SE1	I feel confident in identifying phishing emails							
SE2	I know what to do when I receive a suspicious email							
SE3	I can easily distinguish between a phishing email and a legitimate one							
SE4	I am confident in my ability to avoid falling for phishing scams							
RC1	It takes too much time to verify emails before opening them							
RC2	Reporting phishing emails is a hassle							
RC3	Following email security practices is inconvenient							
RC4	Double-checking email authenticity disrupts my work							

Section 4: Phishing Resilience

No.	Question	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

1	I can recognize suspicious links in emails							
2	I am able to distinguish phishing emails from legitimate ones							
3	I carefully check email sender addresses before opening links or attachments							
4	I avoid clicking on email links unless I'm sure they are safe							
5	I do not download attachments from unknown senders							
6	I always verify unexpected emails before responding or taking action							
7	If I receive a suspicious email, I report it to the IT/security department							
8	I know the correct procedure for reporting phishing attempts at my workplace							
9	I encourage colleagues to report phishing emails when they encounter them							
10	I feel confident in responding appropriately to a phishing attempt							
11	I am sure of what steps to take if I suspect an email is a phishing attempt							

Submitted by:

_____ _____

_____

Student Signature Date

Approved by:

1. _____ _____ _____

Advisor Signature Date

1. _____ _____ _____

Chairman, Signature Date

Deparment's Graduate Committee