TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Vito Pavlica 223596IVCM

HUMAN-CENTERED PHISHING DETECTION

Master's thesis

Supervisor: Ricardo Gregorio Lugo

PhD

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Vito Pavlica 223596IVCM

INIMKESKNE ANDMEPÜÜGITUVASTUS

Magistritöö

Juhendaja: Ricardo Gregorio Lugo

PhD

Tallinn 2025

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Vito Pavlica

17.5.2025

Abstract

This thesis examines employee susceptibility to phishing attacks using a mixed-methods approach that combines behavioral data from a simulated phishing exercise with psychological survey responses. The study explores the extent of phishing vulnerability in organizational settings, the influence of individual psychological factors such as self-efficacy and perceived severity, and the role of organizational training and design in mitigating phishing success rates.

A phishing simulation involving 430 participants revealed high susceptibility across roles, with 57% of emails opened, 46% of links clicked, and 25% of users entering their credentials. Despite assumptions that IT staff would be more resilient, no statistically significant differences were observed across job roles. A follow-up survey measuring perceived vulnerability, response efficacy, and related constructs failed to predict users' behavioral intentions reliably. The internal consistency of several scales was low, and no psychological predictor reached statistical significance.

The findings suggest that traditional cognitive-behavioral models may not fully explain phishing susceptibility and highlight a gap between self-reported security attitudes and actual user behavior. The thesis emphasizes the importance of integrating behavioral simulations into cybersecurity training and advocates for human-centered, experiential learning approaches tailored to diverse organizational roles.

This work contributes to the field of cybersecurity by questioning the effectiveness of conventional self-report frameworks and offering practical guidance for designing adaptive, evidence-based anti-phishing interventions.

This thesis is written in English and is 56 pages long, including 5 chapters, 4 figures and 18 tables.

Annotatsioon

Käesolev magistritöö uurib töötajate vastuvõtlikkust õngitsusrünnakutele, kasutades kombineeritud meetodit, mis ühendab käitumuslikud andmed simuleeritud õngitsusharjutusest ja psühholoogilise küsitluse vastused. Uuring analüüsib õngitsusrünnakute haavatavuse ulatust organisatsioonilises kontekstis, individuaalsete psühholoogiliste tegurite - nagu enesetõhusus ja tajutud tõsidus - mõju ning organisatsioonilise koolituse ja disaini rolli õngitsusrünnakute edukuse vähendamisel.

Simuleeritud õngitsusharjutus, milles osales 430 inimest, näitas suurt vastuvõtlikkust kõikides ametirühmades: 57% avasid e-kirja, 46% klõpsasid lingile ja 25% sisestasid oma mandaadid. Vaatamata eeldustele, et IT-töötajad on vastupidavamad, ei täheldatud ametirühmade vahel statistiliselt olulisi erinevusi. Järgnev küsitlus, mis mõõtis tajutud haavatavust, reageerimisvõimekust ja seotud konstrukte, ei suutnud usaldusväärselt ennustada kasutajate käitumuslikke kavatsusi. Mitmete skaalade sisemine kooskõla oli madal ning ükski psühholoogiline ennustaja ei saavutanud statistilist olulisust.

Tulemused viitavad sellele, et traditsioonilised kognitiiv-käitumuslikud mudelid ei pruugi täielikult seletada vastuvõtlikkust õngitsusele ning toovad esile lõhe kasutajate eneseraporteeritud turvahoia ja tegeliku käitumise vahel. Magistritöö rõhutab käitumuslike simulatsioonide integreerimise tähtsust küberkaitsekoolitusse ning toetab inimkeskseid, kogemuslikke õppeviise, mis on kohandatud erinevatele organisatsioonilistele rollidele.

See töö panustab küberjulgeoleku valdkonda, seades kahtluse alla traditsiooniliste eneseraportil põhinevate raamistikute tõhususe ning pakkudes praktilisi juhiseid kohanduvate, tõenduspõhiste õngitsusvastaste sekkumiste kavandamiseks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 56 leheküljel, 5 peatükki, 4 joonist, 18 tabelit.

List of abbreviations and terms

Abbreviation	Full Meaning
AI	Artificial Intelligence
ANOVA	Analysis of Variance
BI	Behavioral Intention
CFA	Confirmatory Factor Analysis
CI	Confidence Interval
ENISA	European Union Agency for Cybersecurity
EU	European Union
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
PA	Perceived Ability (to detect phishing emails)
PCA	Principal Component Analysis
PMT	Protection Motivation Theory
PS	Perceived Severity
PV	Perceived Vulnerability
RC	Response Cost
RE	Response Efficacy
SD	Standard Deviation
SE	Self-Efficacy
SMS	Short Message Service
SP	Statistical Power
TRAPD	Translation, Review, Adjudication, Pretesting, Documentation
UBA	User Behavior Analysis
URL	Uniform Resource Locator
VIP	Very Important Person
VPN	Virtual Private Network

Table of contents

List of figures

List of tables

1 Introduction

1.1 Background and motivation

Phishing remains one of the most persistent and damaging threats in the cybersecurity landscape. Despite advancements in technical defenses such as spam filters, anomaly detection systems, and endpoint protection, phishing continues to exploit a much harder-to-secure element: the human. Attackers routinely capitalize on cognitive biases, emotional triggers, and varying levels of cybersecurity literacy to manipulate users into taking harmful actions, such as clicking malicious links or revealing sensitive information (Curtis et al., 2018; Jari, 2022).

The financial impact of phishing is substantial and growing. According to IBM's 2024 Cost of a Data Breach Report, the average cost of a phishing breach reached $4.88 million, marking a nearly 10% increase from the previous year (IBM, 2024). Beyond direct financial losses, organizations suffer from operational disruptions, reputational damage, and decreased employee productivity. For instance, the cost of lost productivity due to phishing attacks ballooned from $1.8 million in 2015 to $3.2 million per company in 2021 (Ponemon Institute, 2021).

Phishing attacks are also becoming more sophisticated. In 2024, there was a significant increase in phishing messages, with a notable surge in credential-based phishing attacks (Zscaler, 2024). The rise of AI-generated phishing scams has further exacerbated the issue, enabling attackers to craft highly personalized and convincing fraudulent emails that are more likely to deceive recipients (Eze & Shamir, 2024).

The human element of cybersecurity is found to be increasingly focused on, to mitigate these threats. Effective strategies include continuous security awareness training, simulated phishing exercises, and the implementation of behavioral analytics to identify and address risky behaviors (HIPAA Journal, 2022). Programs of gamified training have been showing big promises in enhancing user engagement and improvement of the ability to recognize and respond to phishing attempts (Rahartomo et al., 2025). By addressing the human factors in relation with phishing attacks, organizations' overall cybersecurity posture can be strengthened, and the likelihood of successful breaches can be reduced.

The motivation behind this thesis is the growing need to explore human-centered solutions to phishing attacks. Rather than focusing solely on technical countermeasures, this study investigates why individuals fall for phishing attempts and how those vulnerabilities can be mitigated through tailored, behaviourally informed interventions. By understanding the psychological and contextual elements that influence user decision-making, organizations can better design training programs and system interfaces that support safer behaviour.

1.2 Problem statement

While technical defenses are essential, they are insufficient to combat phishing threats that manipulate human behavior. Phishing continues to succeed not because of a lack of technological capability, but due to gaps in human awareness, attention, and behavior. There is a lack of comprehensive understanding of how factors like cognitive biases, stress, and varying levels of cybersecurity knowledge affect users' susceptibility to phishing emails in real organizational environments. Moreover, the effectiveness of training and human-centered design in addressing these issues remains underexplored in practical settings.

1.3 Research questions

This thesis is guided by the following research questions:

- RS1: What are the overall success rates of email-based phishing simulations in organizational settings, and how do these rates relate to phishing susceptibility?
- RS2: How do individual cognitive biases and cybersecurity literacy levels affect susceptibility to phishing attempts?
- RS3: What organizational measures, such as staff training and system design, might effectively lower the success rate of phishing attempts in a controlled simulation setting?

1.4 Scope of the study

This study focuses specifically on email-based phishing in organizational environments. It does not include social media phishing, voice phishing (vishing), or smishing (SMS phishing). The research excludes technical mechanisms such as spam filters or algorithmic detection systems, focusing instead on the human variables that influence phishing susceptibility.

A range of organizational roles are represented in the study-including IT staff, administrators, finance personnel, and executives-to provide a comprehensive view of phishing vulnerability across departments. Controlled simulations are used to replicate real-world phishing attacks, accompanied by surveys and interviews to capture both quantitative and qualitative data.

1.5 Structure of the thesis

The remainder of the thesis is organized as follows:

- **Introduction:** Contextualizes phishing risk, states research questions, and outlines contributions.
- **Literature Review:** Surveys psychological, behavioral, and organizational work on phishing susceptibility.
- **Methodology:** Describes the mixed-methods design: industry-tailored phishing simulations, survey development, and analytic procedures.
- **Results:** Reports behavioral metrics (open, click, credential rates), survey descriptives, reliability analyses, and regression outcomes.

- **Discussion and conclusion:** Interprets findings, directly answers RQ1-RQ3, examines the intention-behavior gap, and draws theoretical and practical implications. Also summarizes key insights, emphasizes contributions, and points to future research directions.
- **References & Appendices:** Lists sources and includes the consent form.

2 Literature review

This research review examines the behavioral and psychological aspects of phishing vulnerability, the efficacy of educational and training interventions, and the role of organizational measures in mitigating phishing risks by concentrating on human weaknesses. The review's objective is to find weaknesses in current strategies and offer practical suggestions for enhancing phishing prevention by analyzing recent research. This human-centered approach delivers a thorough understanding of phishing and lays the groundwork for creating all-encompassing solutions to one of cybersecurity's most enduring problems by fusing quantitative data with qualitative insights.

Phishing, which targets both individuals and businesses by taking advantage of human weaknesses, is still one of the most pervasive and significant cyber threats. Phishing relies primarily on social engineering - manipulating individuals into revealing sensitive data such as login credentials, PINs, or financial details - rather than exploiting software or system vulnerabilities (Chrysanthou et al., 2023; Khadka et al., 2024). Phishing tactics have become more challenging to identify because of their constant improvements, which avoids both automatic detection systems and human probe (Darktrace, 2023; Eze & Shamir, 2024). Billions of dollars of losses are generated through phishing attacks, and they affect individuals, corporations, governments and others. According to the 2024 IBM Cost of a Data Breach Report, the average cost of a phishing breach reached $4.88 million, marking a nearly 10% increase from the previous year (IBM, 2024). Furthermore, phishing attacks accounted for 36% of all U.S. data breaches in 2023 (Verizon, 2023). Beyond monetary losses, these attacks cause companies to face legal issues and provide harm to their reputation, underscoring their extensive consequences. Even with better automated filters and anomaly detectors in place, people remain the weakest link in phishing defense-highlighting because we need a strategy that puts human behavior at its center (Moustafa et al., 2021).

To address the persistent vulnerabilities posed by human behavior in phishing attacks, recent European regulatory frameworks and expert guidelines have emphasized mandatory security awareness and behavior-focused training. The European Union's Directive (EU) 2022/2555, which is also known as NIS2, requires that all essential and important entities within the European Union implement regular and role-specific cybersecurity training for employees and members of management bodies (European Union, 2022). In Article 20 of the directive, it is explicitly stated that organizations need to adopt core cyber-hygiene practices and boost people's understanding of phishing and other online threats through regular, hands-on training and drills. This reflects a broader recognition that technical controls alone are insufficient if users continue to fall prey to socially engineered attacks. Complementing this regulatory obligation, the European Union Agency for Cybersecurity (ENISA) provides actionable guidance on how to effectively implement these training requirements. ENISA emphasizes that rather than one-off, generic, monotonous sessions, the programs for organizations should be more ongoing and hands-on. Realistic phishing drills, regular check-ins and active learning methods should be used to see how people behaviors are evolving (ENISA, 2021). The guidelines further recommend segmenting training by role and risk exposure, as well as

aligning content with cognitive psychology insights, such as users' susceptibility to authority, urgency, and attentional fatigue. Another argument from ENISA is that trainings success should be judged by actual behavior, not just remembrance. This way security awareness should become part of day-to-day culture, rather than just a compliance task. If the NIS2 and ENISA's guidance are paired it marks a clear move towards highlighting human factors as the heart of cybersecurity. IT also gives recognition to the psychological and situational drivers of phishing risk, while calling for systematic safeguards to address them.

An analysis of human behavior and decision-making is necessary to comprehend why phishing assaults persist even in settings with strong technical barriers. Phishing attacks often exploit psychological strategies such as urgency, authority, and scarcity to manipulate individuals into compromising actions (Hadnagy, 2018). These tactics work especially well in workplaces with lots of stress, where default habits are norm, because of it and employees do not pause for careful thought (Curtis et al., 2018). People tend to rely on automatic responding, rather than thinking clearly and analytically while reasoning- this speeds decision making while also making them much more prone to errors (Porcelli & Delgado, 2017). This shift can result in employees prioritizing efficiency over caution, making them more susceptible to phishing attempts. Stress can weaken our focus and recall, which makes it harder to spot the warning signs of phishing-email addresses that are not correct or have a changed letter or maybe weird, phrased sentences (Starcke & Brand, 2012). Keeping these mental effects in mind is key to designing phishing defenses that really work for people.

When we are stressed or exhausted, our decision-making weakens, and we become more likely to fall for phishing emails. Stress overloads our cognitive system and limits the attention and analytical thinking needed to spot unusual URLs or unfamiliar sender addresses (Starcke & Brand, 2012). In a simulated exercise, people under high stress were much more prone to click on phishing links (Zhuo et al., 2024). Prolonged work demands can also lead to emotional exhaustion, draining mental energy, reducing vigilance, and encouraging impulsive actions. Research shows that emotionally exhausted individuals make poorer decisions, increasing their risk of online scams (Wen et al., 2022). These vulnerabilities worsen when employees lack hands-on cybersecurity training and real-world practice, leaving them unprepared to recognize and respond to phishing attacks.

Even though tools like spam filters or endpoint detections systems are crucial to help us stop phishing, they do not address the cognitive and behavioural flaws that are exploited by attackers (Huang et al., 2021). Phishing attacks often leverage psychological tactics-such as urgency, authority, and fear-to manipulate individuals into bypassing logical decision-making processes. The unpredictability of these human factors cannot be fully mitigated by automated systems (Arevalo et al., 2023).

Phishers keep tweaking their tactics to slip past automated defenses. For example, zero-day phishing attacks often sail right through spam filters until the systems catch up and learn to block them (Arevalo et al., 2023). Additionally, sophisticated phishing campaigns may use personalized information gathered from social media or previous breaches to craft convincing messages that are difficult for both users and automated systems to detect (Kavvadias & Kotsilieris, 2025).

Human-centric approaches must complement technological defenses, they should both be thought of as critical components. These should include regular security awareness training, simulated phishing exercises, and fostering a culture of vigilance to effectively reduce the risk of successful phishing attacks (Arevalo et al., 2023).

Phishing attacks are successful because they take advantage of several behavioral and psychological traits, while also exploiting social and organizational aspects. . When people evaluate risks based on immediate and accessible examples, cognitive biases like the availability heuristic cause them to underestimate phishing hazards if they haven't directly seen them (Alsharnouby et al., 2015). Furthermore, those who believe they are less likely to fall for frauds tend to become overconfident and less vigilant, which increases susceptibility due to the illusion of invulnerability (Downs et al., 2006). Emotional cues are another cornerstone of phishing schemes. By playing on curiosity, fear, or urgency, attackers push people to react without pausing to think. For example, subject lines like "Account Suspended" or "Immediate Action Required" are designed to short-circuit logical decision-making and get you to click first, ask questions later (Sheng et al., 2017).

Phishing susceptibility is influenced by a complex interplay of psychological, situational, and demographic factors. Situational diversions and workplace stress can exacerbate psychological vulnerabilities, leading employees to prioritize task completion over security checks. This tendency increases their susceptibility to phishing attacks. The shift to remote work environments has further compounded these challenges, as employees often multitask and navigate blurred lines between personal and professional responsibilities, making it more difficult to recognize potential threats (Caputo et al., 2016; Jensen et al., 2017).

Age and cybersecurity expertise both shape how likely someone is to fall for phishing. Younger people often feel sure they can spot a scam, while older adults may not be up to speed on the latest tricks-either way, the result is more risk (Lin et al., 2019). That's why researchers now say we need training that fits each generation's habits and challenges. Take Gen Y, for example: they're good about keeping antivirus software current. Gen Z, on the other hand, often feels so confident they skip those routine updates (Debb et al., 2020).Moreover, integrating behavioral analytics into phishing detection systems can enhance real-time threat identification. By analyzing user activity patterns, such as unusual click sequences or atypical login times, organizations can more accurately identify potential phishing attempts. This approach not only improves detection but also informs the development of more targeted and effective training interventions (CybSafe, 2022).

A comprehensive strategy that includes psychological understanding, generational differences consideration and behavioural analytics, should be used to address the multifaceted nature of phishing susceptibility. Customized training programs that reflect these elements can significantly bolster an organization's defense against phishing attacks. (Lin et al., 2019).

Since they directly target human vulnerabilities that technology solutions cannot completely avoid, effective training and educational interventions are essential for lowering vulnerability to phishing attacks. Although traditional approaches like lectures and static manuals offer foundational knowledge, they often fall short in actively engaging staff members, thereby diminishing their effectiveness (Alshaikh, 2020). Research indicates that students in traditional lecture-based courses are 1.5 times more likely to fail compared to those in active learning environments, and active learning strategies have been shown to increase exam scores by approximately 6% over traditional lectures (Freeman et al., 2014).Interactive training techniques, such as phishing simulations, have demonstrated significantly greater effectiveness in enhancing employees' ability to identify and avoid phishing attempts compared to traditional methods (Jampen, et al, 2020). A comprehensive study by KnowBe4, analyzing data from

over 60,000 organizations and more than 32 million users, revealed that organizations implementing both regular security awareness training and frequent simulated phishing tests achieved up to a 96% improvement in users' ability to detect phishing emails (Grimes & Kraemer, 2023). These simulations provide employees with practical experience in recognizing phishing tactics within a controlled environment, thereby reinforcing learning and promoting cautious behavior when interacting with unfamiliar communications.

Everyone talks up custom phishing training, but the latest research offers a more balanced view. In a large meta-analysis, Prümmer et al. (2024) showed that cybersecurity training does improve user behavior, with a strong effect size ($d = 0.75$), especially when programs assess behavior in real-world settings. This makes it clear that training must include behavioral insights if we want it to change habits.

On the other hand, Lain et al. (2024) evaluated training that is built into employees' daily routines by sending fake phishing emails and then offering immediate instruction to anyone who clicks on them. Their results indicate that the main benefit comes from nudging people with regular reminders of potential threats rather than from the training content itself. Many employees skip the instructional material, citing time pressures or a sense that it is not useful. In this study, repeated exposure led to a small but meaningful improvement in behavior (effect size $d = 0.34$), suggesting that frequent prompts are more effective than detailed lesson plans.

These contrasting findings highlight the complexity of designing effective cybersecurity training programs. To reconcile these discrepancies, organizations should consider implementing multifaceted training strategies that combine behavioral insights with practical engagement methods. Incorporating real-time feedback, diverse training formats, and gamification elements can enhance engagement and retention. Moreover, embedding cybersecurity awareness into the organizational culture, rather than treating it as a one-time event, reinforces its importance and encourages continuous learning (Parsons et al., 2014).

Another key step is to use behavioral analytics in phishing detection tools so they can spot threats in real time. When organizations review user activity (for example, click patterns that look out of the ordinary or logins at unusual hours), they can flag phishing attempts with greater accuracy. This approach makes security measures both proactive and quick to adapt as cybercriminals try new tactics (Sahingoz et al., 2019).

While training programs are instrumental in enhancing cybersecurity awareness, they are not without limitations. Over time, issues such as training fatigue and desensitization can diminish their effectiveness, particularly when simulations or instructional materials become monotonous or overly generic (Reeves et al., 2021). This phenomenon, known as security fatigue, leads to decreased vigilance and engagement among employees, making them more susceptible to phishing attacks (Nobles, 2022).. To address these challenges, incorporating personalized and engaging interventions is crucial. For instance, Barz et al. (2024) demonstrated that a symptom-titrated exercise program significantly reduced fatigue levels among participants, highlighting the importance of individualized approaches in maintaining long-term effectiveness. Similarly, integrating real-time feedback, diverse training formats, and gamification elements can enhance engagement and retention of cybersecurity practices (Alsharnouby et al., 2015). Embedding cybersecurity awareness into the organizational culture, rather than treating it as a one-time event, further reinforces its importance.

Leaders set the stage for security across the entire organization, which is essential to building a strong cybersecurity culture (Brigantia, 2024). When managers explain clearly why protecting information matters, employees feel responsible for safeguarding assets. Alshaikh (2020) argues that the most effective cybersecurity processes blend individual behavior with company culture. It is equally crucial to equip staff with the tools and systems they need to spot and report phishing attempts. By offering reporting channels that are easy to use and encouraging prompt alerts about anything suspicious, organizations strengthen their defenses and speed up threat response.

Additionally, Alsharnouby et al. (2015) emphasize the importance of continuous employee engagement, highlighting that organizations with established incident response procedures are more adept at neutralizing threats before they escalate. Beyond incident response, several organizational factors play a pivotal role in strengthening cybersecurity culture. Leadership commitment is paramount; when leaders actively promote and model security-conscious behaviors, it sets a precedent for the entire organization (Delso-Vicente et al., 2025). Regular training and awareness programs tailored to various employee roles ensure that staff remain informed about evolving threats and best practices. Moreover, fostering open communication channels encourages employees to report suspicious activities without fear, enhancing the organization's ability to respond promptly to potential incidents (Corradini, 2020). By integrating these organizational strategies, companies can cultivate a proactive security posture that extends beyond technical defenses.

Bringing technical defenses together with human-focused measures creates a layered security approach that stands up better to phishing. Tools like intrusion detection systems and email filters are vital, but they cannot catch every threat. When they are paired with comprehensive staff training, organizations address both machine and human weaknesses. Jampen and colleagues (2020) found that adding regular, simulated phishing exercises to existing technical safeguards led to a marked drop in successful attacks. Specifically, over a 63-day period, the failure rate among employees who received embedded training decreased to 24.5%, compared to 32.08% for those who only received feedback and 47.5% for those without any training or feedback.

The significance of cooperation between technical and human-centered defenses is further underscored by Jensen et al. (2017), who found that organizations employing AI-enhanced monitoring systems in combination with human oversight demonstrated improved phishing detection rates. A stronger barrier against cyberthreats is produced through the integration of technological defenses and user-focused strategies. While technical safeguards such as spam filters and endpoint detection systems are essential, they alone are insufficient to prevent phishing attacks. Regular phishing simulations can be used as a critical complement by actively engaging employees in real-life scenarios, helping them practice identifying and responding to deceptive emails in a safe environment (Parsons et al., 2019).

Heiding et al. (2024) found that phishing emails generated entirely by AI achieved a 54 % click-through rate, matching messages created by human specialists. When a human review step was added that rate climbed to 56 %, underscoring how these attacks are becoming both more sophisticated and more personalized. These findings emphasize that fostering user vigilance through practical training, in conjunction with robust technical infrastructure, leads to significantly enhanced detection and mitigation of phishing attacks.

The foundation of strengthening vigilance against phishing is the establishment of explicit policies and processes. Mandatory reporting procedures foster an initiative-taking security environment by ensuring that staff members are aware of what to do if they receive questionable emails. But sticking to these guidelines can be difficult, particularly as phishing techniques change. Employees must get ongoing training and policy changes on a regular basis to stay knowledgeable about emerging risks. Jensen et al. (2017) stress that for policies to continue to be effective, they must be flexible and dynamic, considering the evolving nature of cyberthreats. Additionally, companies that include phishing simulations in routine evaluations offer beneficial chances to improve these rules considering vulnerabilities found (Lin et al., 2019).

Phishing powered by AI has transformed how attackers operate, making their campaigns more sophisticated and dangerous. By feeding large datasets into machine learning models, they craft messages that play on each target's unique weaknesses and interests. Some even use deep-fake voices or avatars to impersonate trusted individuals, which makes their requests seem even more believable (Heiding et al., 2023). These advances put traditional, rule-based filters at a serious disadvantage because they struggle to keep up with such clever, ever-changing tactics (Basit et al., 2021). What's worse, once set up, an AI-driven phishing system can send thousands of highly tailored emails in just minutes, vastly outpacing human attackers (Vishwanath et al., 2018).

Although phishing simulators are still a vital component of organizational training, there are unstated expenses associated with their use that may reduce their efficacy. Employees may experience needless stress because of poorly designed simulations, especially ones that imitate emotionally delicate situations like financial hardship or personal issues. According to studies, simulations that are viewed as dishonest or harsh may cause employee confidence to erode, which will lower participation in cybersecurity initiatives (Bada et al., 2019). To prevent unfavourable results, organizations must create simulations that are both difficult and mindful of workers' welfare. This balance has been successfully attained by customizing simulations to mimic actual phishing techniques while preserving ethical transparency (Graf, 2023).

Using phishing simulators raises important ethical questions, especially around being open with employees and getting their informed consent. Resnik and Finn (2017) argue that we need to balance an organization's security needs with workers' rights to privacy and respect. Rather than creating fear or resentment, a clear ethical approach helps build trust and fosters a learning mindset. It also keeps pushback to a minimum when staff understand why these exercises are happening and what their goals are. Basit et al. (2021) found that companies using transparent, no-blame training see higher engagement from employees and better adherence to security policies.

Bringing technical defences together with insights into how people behave makes phishing protection far more effective. By watching for odd patterns-like users clicking through a strange sequence of links, logging in at unusual hours, or veering off normal navigation paths-organizations can spot attacks as they happen. This method, often called User Behavior Analytics or UBA, looks for signs that an account may be compromised (Sánchez-Rola, Dell'Amico, & Balzarotti, 2020). For example, Varonis (2022) shows how UBA tracks everything from which applications someone opens to their file-access habits, so any change from the norm raises an alert. RocketMe Up Cybersecurity (2024) makes a similar point, explaining that defining what "normal" looks like and then flagging deviations is key to staying ahead of threats. Machine learning drives these systems forward by learning from user interactions and adapting to new phishing tricks. Take PhishNet, which uses XGBoost to blend behavioral signals with advanced modeling and

achieve strong accuracy in spotting fake websites (Kumar et al., 2024). Research also shows that systems which adapt in real time-examining both how users respond and the metadata in incoming emails-can catch the smallest irregularity that rule-based filters miss (Sheng et al., 2017). By combining data-driven alerts with human judgment, these solutions do not just detect threats better, they also give security teams clear, actionable insights for stopping attacks.

Future studies on phishing protection need to consider how sophisticated attacks are becoming, especially those powered by artificial intelligence (AI). Attackers are using AI increasingly to create highly customized emails, which presents problems for human awareness and detection systems (Basit et al., 2021). Training frameworks must change in tandem with these innovative strategies to combat these dangers. For example, phishing prevention results could be enhanced by customized training programs that adjust to the unique behaviors and learning requirements of each user (Jensen et al., 2017). Additionally, employees now face more distractions and a blurring of the lines between work and home activities due to the growing popularity of remote and hybrid work environments. According to Salahdine et al. (2022), customized phishing detection methods and flexible security measures are required to oversee the unique dangers connected to these work types.

Improving the user experience of security tools is vital to ensure they are widely adopted and effective. When interfaces are clear, reduce mental strain, and provide timely alerts, people make fewer mistakes and rely on them more. In fast-paced work environments it is important to balance efficiency with robust security. Alshaikh (2020) argues that tools which fit seamlessly into daily workflows are more likely to gain user acceptance and be used effectively. Involving employees in the design and rollout of security measures helps build a proactive security culture and ensures the solutions not only work well but also boost staff satisfaction.

The studied literature emphasizes how persistent phishing assaults are, especially when it comes to their use of social engineering and psychological manipulation to take advantage of human weaknesses. People are vulnerable to phishing efforts because of cognitive biases like urgency bias and faith in authority, as well as emotional states like stress and exhaustion (Sheng et al., 2017). Situational factors including job interruptions and the growing sophistication of phishing attempts further increase this vulnerability. The data shows that although technical fixes are necessary, they are not enough to overcome these ingrained psychological weaknesses. This emphasizes how crucial it is to take a human-centered approach to cybersecurity frameworks, incorporating organizational tactics, educational programs, and psychological insights.

Education and training interventions are vital for lowering phishing risks. Hands-on exercises and behavioral practice, such as phishing simulations, have strengthened employee resilience (Jampen et al., 2020). Yet traditional methods can lead to fatigue and reduced sensitivity over time, so we need approaches that adapt to each learner. By using data driven insights, training tailored to people's specific roles and habits can boost effectiveness while keeping them engaged (Alshaikh, 2020; Jensen et al., 2017). Still, questions remain about how well these methods hold up against ever more sophisticated phishing attacks, especially those enhanced by artificial intelligence.

To bridge the gap between technology and human defenses, organizational techniques are essential. It has been demonstrated that a strong cybersecurity culture, supported by clear communication, leadership, and encouraging policies, enables staff members to take an active role in organizational security (Alsharnouby et al., 2015). A multi-layered defense

against phishing threats can be achieved by combining technical tools with human-centered initiatives, such as regular simulations and real-time reporting mechanisms (Jampen et al., 2020). However, issues like making sure regulations are followed, adjusting to new threats, and striking a balance between security precautions and employee trust continue to be obstacles.

Today's threat landscape keeps evolving, driven by AI-powered phishing schemes, the hidden costs of running simulations, and tough ethical questions. With AI, attackers can now design highly believable, personalized phishing campaigns that outsmart both people and automated defenses (Basit et al., 2021). At the same time, we must balance security goals with employee well-being. That means building training programs that are transparent fair and free of punishment (Resnik & Finn, 2017). To meet these challenges, we need an all-in approach-one that blends behavioral insights with cutting-edge technical safeguards and holds fast to strong ethical standards.

There are still a lot of gaps in literature despite tremendous advancements. Numerous studies highlight the usefulness of training in the short term while ignoring its long-term effects and scalability. Further research is necessary because the study of phishing vulnerability in remote and hybrid work contexts is still in its initial stages (Salahdine et al., 2022). To create thorough prevention methods, this review emphasizes the necessity of interdisciplinary approaches that integrate knowledge from organizational behavior, psychology, and cybersecurity.

3 Methodology

This chapter explains how we investigated people's vulnerability to phishing in workplace environments. Because phishing susceptibility involves many factors, we combined methods to capture both what people do and how they think. First, we ran phishing simulations to see how participants responded to fake attacks. Then we asked them to complete an online questionnaire about their cybersecurity attitudes, perceptions, and self-reported habits. By pairing real-world behavior with survey insights into cognitive, emotional, and situational factors, this approach gives us a full picture of why people fall for phishing.

3.1 Research design

We designed the study as a convergent mixed-methods project, collecting behavioral data and survey responses at the same time and then looking at both together. This lets us compare what people do with what they say they believe - and it boosts confidence in our results (Fetters, Curry, & Creswell, 2013).

In the phishing simulation, we recorded real actions, for example who clicked or tried to log in. The survey then added context by asking participants to rate how severe they thought phishing was, how confident they felt about spotting it, and how much they knew. That combination is ideal for phishing research because people often do one thing but say another, this is what experts call the "intention-behavior gap."

This design is aligned with the research objectives and questions. Specifically:

- RQ1 (success rates of phishing simulations) is addressed through behavioral tracking,
- RQ2 (influence of cognitive biases and literacy) is explored via validated scales,
- RQ3 (organizational interventions) is supported by cross-sectional insights gathered before awareness training.

3.2 Participants and context

Participants were recruited from multiple organizations, each operating in different sectors and of varying sizes. This diversity increases the ecological validity of the findings and allows for the examination of phishing susceptibility across a range of organizational environments.

A power analysis was conducted using G*Power (Faul et al., 2007) to determine the minimum required sample size for a multiple linear regression analysis. The analysis assumed a medium effect size ($f^2 = 0.15$), significance level of $\alpha = 0.05$, desired power of 0.90, and 3 predictors.

The results indicated that a minimum of 77 participants would be required to detect an effect of this size with adequate statistical power. Given that the present study included 108 valid responses, the sample size was sufficient to detect medium-sized effects in the regression models.

Table 1:G*Power a priori power analysis for multiple linear regression

Parameter	**Value**
Test type	Linear multiple regression (Fixed model, R^2 increase)
Statistical power (1 - β)	0.90
Significance level (α)	0.05
Effect size (f^2)	0.15 (medium)
Number of predictors	3
Required sample size	**77**

All employee roles were eligible for inclusion, including but not limited to IT professionals, administrative staff, HR personnel, finance departments, and management. This broad inclusion criterion supports the aim of evaluating phishing susceptibility across organizational hierarchies and functional domains.

Phishing simulations were carried out remotely, and the questionnaire was administered online using the 1ka.arnes.si platform. Importantly, the questionnaire was distributed prior to any cybersecurity education, enabling an authentic measure of baseline attitudes and awareness.

3.3 Phishing simulation procedure

Phishing simulations were conducted using the open-source platform GoPhish, which allows for the creation and management of customized phishing campaigns, as well as detailed tracking of user interactions. Each participating organization received a tailored phishing email, developed in consultation with its IT department and designed according to the NIST Phishing Framework (NIST SP 800-177).

The emails incorporated known psychological manipulation techniques, such as urgency, authority, scarcity, or curiosity. Specific triggers varied based on organizational context and were aligned with common phishing tactics defined in existing standards. Examples include fake password reset requests, spoofed messages from HR, or shipping notifications.

Each simulation lasted for 24 hours, beginning at 09:00 on the launch day and concluding at 09:00 the next day. During the simulation, three key actions were tracked:

1. Click rate - whether the participant clicked the embedded link,
2. Page visit - whether the participant viewed the phishing landing page,
3. Credential entry - whether the participant entered any sensitive information.

Participants were not notified in advance of the simulation to preserve realism. Only organizational IT administrators were aware of the test, ensuring operational security and proper oversight.

3.4 Phishing e-mail design

To bring our methodology to life and demonstrate its real-world relevance, we provide a rich, narrative account of the phishing emails used in the simulation. Each message was carefully designed to resemble genuine internal communications, complete with the organization's actual logo, colour palette, and familiar signoffs. We constructed scenarios around everyday tasks such as password resets, software updates, and calendar invitations, invoking real department heads or IT staff to lend credibility and authority to each message. By describing the exact wording, visual layout, timing, and emotional triggers embedded in these mock attacks, we offer a behind-the-scenes view of the psychological strategies at play (Hadnagy, 2018). This story-driven approach allows us to identify precisely which cues led participants to click immediately and which elements prompted further scrutiny. Framing our methods in this narrative style not only enhances transparency but also strengthens the ecological validity of our study, helping us understand how and why different employee groups respond to specific phishing tactics (Workman, 2008).

3.4.1 Company #1 - Logistics

The first phishing email contained thirteen identifiable cues. This places it in the Some cues tier of the NIST Phish Scale framework, indicating a moderate presence of potential warning signs (NIST, 2021). Major contributors included three examples of misleading link text that hid the true URL, one instance of implied time pressure, a missing branding element, and minor grammatical inconsistencies. Despite these indicators, the overall tone remained polished enough that users with limited phishing awareness could easily overlook the warning signs.

A separate assessment of premise alignment produced a score of twelve, corresponding to a medium relevance rating. This shows the phishing message borrowed elements of genuine workplace correspondence, such as references to common business processes and simulated communication from a supervisor (Workman, 2008). However, small deviations from the company's usual communication style prevented it from achieving a higher level of authenticity.

When combined, the Some cues rating and medium premise alignment result in an overall classification of Moderately Difficult for detection. This balance between realistic presentation and challenge ensures the email tests natural user responses without making detection too simple or unrealistically hard. Maintaining this balance is crucial for ecological validity in phishing simulation research and for accurately reflecting typical vulnerabilities within the organizational environment.

Table 2: NIST Phishing scale classification for Company #1

Aspect	**Result**
Cues Detected	Some (13 cues)

Premise Alignment	Medium (score 12)
Detection Difficulty	Moderately Difficult

The phishing scenario for the first company was designed to simulate credible internal communication from the organization's IT department. The phishing email informed employees of an urgent requirement to enhance the security of remote access services by downloading a new VPN provider application and setting up two-factor authentication (2FA).

The message used official-sounding language and adopted the typical tone and structure of legitimate IT communications, including references to cybersecurity policies and procedural compliance. A hyperlink embedded in the message redirected users to a phishing site that closely mimicked the official Microsoft login portal, complete with branding and familiar design elements. Users were prompted to enter their corporate credentials as part of the "new security setup" process.

This scenario was selected to exploit common trust in internal IT communications and procedural compliance pressure, both of which are known psychological factors that influence user behavior in phishing attacks (Hadnagy, 2018; Workman, 2008). By replicating a standard security update procedure, the email increased plausibility and reduced suspicion, thereby providing a realistic test of employees' phishing detection abilities in a critical operational context.

3.4.2 Company #2 - Music industry

The second phishing email exhibited a total cue count of 14, placing it within the "Some" cues category according to the NIST Phish Scale framework. This categorization indicates a moderate number of detectable phishing indicators embedded within the email. Key features contributing to the cue count included mismatches between the sender's name and email address, the use of a plausibly similar domain name, hidden hyperlink destinations, and the presence of an imitation branding element. Additional cues such as minor grammatical errors, the use of time pressure, and requests for sensitive information further enhanced the credibility of the phishing attempt. Despite these indicators, the email maintained a relatively professional appearance, which could increase the difficulty of detection for less experienced users.

The alignment check gave the email a score of twelve, placing it in the Medium relevance bracket. In other words, the message included several hallmarks of genuine workplace communication-tying into current events and using business-related language-but it fell short in mirroring formal company processes and failed to convey meaningful consequences for ignoring the request. Those gaps slightly undercut its overall believability.

Combining the "Some" cue category with a "Medium" premise alignment led to an overall classification of "Moderately Difficult" for phishing detection difficulty. The email was intentionally designed to replicate a realistic phishing scenario that would challenge participants without making detection either too obvious or overly obscure. This approach was crucial for maintaining ecological validity, ensuring that the simulation accurately reflected the kinds of phishing threats employees might encounter in a real-world organizational environment.

Table 3: NIST Phishing classification for Company #2

Aspect	Result
Cues Detected	Some (14 cues)
Premise Alignment	Medium (score 12)
Detection Difficulty	Moderately Difficult

The phishing scenario for the second company was crafted around a real upcoming event to enhance the plausibility of the attack. Employees received an email invitation to a concert, allegedly sent by one of the company's trusted external partners. The message offered VIP access and free tickets to the event, creating an enticing incentive that could easily lower recipients' suspicion.

The email was designed to appear as if it originated directly from the event organizer, using a sender name and branding closely resembling that of the legitimate partner. Embedded within the email was a button labelled to claim the free tickets. Upon clicking the button, users were redirected to a phishing site that mimicked a Google login page, where they were prompted to enter their credentials to "confirm their identity" and complete the ticket reservation process.

This scenario exploited emotional appeal (excitement, exclusivity) and trust in established external relationships, both of which are recognized social engineering tactics that increase susceptibility to phishing attacks (Parsons et al., 2015; Hadnagy, 2018). By leveraging a real event and trusted partner framing, the phishing email increased its contextual relevance and decreased immediate scepticism among recipients, providing a realistic and targeted phishing simulation.

3.4.3 Company #3 - Gas industry

The third phishing email exhibited a total cue count of 14, placing it within the "Some" cues category according to the NIST Phish Scale framework. This categorization indicates a moderate number of detectable phishing indicators embedded within the email. Key features contributing to the cue count included the use of a plausibly similar domain name, missing branding elements, unprofessional formatting, and hidden hyperlink destinations. Further, minor grammar errors, the presence of inappropriate security indicators, and multiple requests for sensitive information were noted, enhancing the deceptive nature of the message. Although these cues were present, the email still maintained enough familiarity in structure and tone to pose a realistic threat, especially to users with only moderate phishing awareness.

The premise alignment assessment produced a score of 14, positioning the email in the "Medium" relevance category. This rating suggests that the phishing attempt was relatively successful in mimicking typical workplace communication processes and showed significant workplace relevance. However, lower alignment with external events and the absence of strong consequences for non-compliance reduced its authenticity to some extent, preventing a higher classification.

Putting together the Some cues designation and the Medium premise alignment results in an overall Moderately Difficult rating for detecting this message. We designed the email to look like a genuine organizational threat while intentionally weaving in small

inconsistencies that test participants' detection skills. Achieving this balance is essential for ecological validity because it ensures our findings accurately reflect how people respond to phishing in everyday work situations.

Table 4: NIST Phishing classification for Company #3

Aspect	**Result**
Cues Detected	Some (14 cues)
Premise Alignment	Medium (score 14)
Detection Difficulty	Moderately Difficult

The phishing scenario for the third company simulated an internal compliance request originating from the organization's legal and human resources departments. Employees received an email informing them of new regulatory requirements, specifically referencing compliance with the NIS2 Directive, and were instructed to update their personal information accordingly.

The email directed recipients to log in via the organization's internal employee portal, with a hyperlink that led to a phishing site mimicking the legitimate portal's design and branding. Upon accessing the site, users were asked to provide sensitive personal information, including their tax identification number and date of birth, under the pretext of updating compliance records.

We crafted this scenario to tap into employees' routine knowledge of internal administrative workflows and the authority they assign to legal and HR notices. By invoking the current NIS2 Directive and emphasizing compliance obligations, the email gained a convincing air of authenticity and urgency. These methods reflect classic social engineering tactics that rely on organizational trust and the fear of falling out of compliance to draw sensitive information from targets (Workman, 2008; Parsons et al., 2015).

3.4.4 Company #4 - Public utility services

The fourth phishing email contained thirteen identifiable cues, which places it in the Some cues tier of the NIST Phish Scale framework (Dawkins & Jacobs, 2023). These cues included a domain name that closely resembled the real one, missing branding elements, minor spelling and grammar mistakes, hidden hyperlink destinations, and inappropriate security icons. The message also asked for sensitive information, applied subtle time pressure, and hinted at consequences, all of which are common tricks to sway user behavior. Even so, the email's polished format and professional tone could easily fool recipients who are not on high alert.

When we evaluated how closely its premise aligned with actual workplace communications, the email scored fourteen-landing in the medium relevance category. This shows it successfully borrowed familiar office language and scenarios, making it feel like a genuine request. However, it did not tie into any external events, nor did it clearly outline immediate repercussions for ignoring the message, which slightly weakened its overall authenticity.

Putting together the Some cues rating with the medium premise alignment gives this message a Moderately Difficult difficulty classification. We designed it to mirror the

nuanced strategies real attackers use in corporate settings, forcing participants to look closely for the tell-tale signs of deception. By striking this balance, the simulation maintains ecological validity and offers a realistic test of how employees detect phishing attempts in their everyday work environment.

Table 5: NIST Phishing classification for Company #4

Aspect	**Result**
Cues Detected	Some (13 cues)
Premise Alignment	Medium (score 14)
Detection Difficulty	Moderately Difficult

The fourth company's phishing scenario took the form of an urgent notice from the Information Technology department. Staff were told that, to meet newly established ISO standards, they must update their user profiles without delay. The message stressed that this step was critical for accurate tracking and management of IT service requests, presenting it as essential for preserving service quality and ensuring compliance.

Recipients were then asked to sign in with their company credentials by following a link. That link led to a counterfeit site designed to look exactly like the organization's genuine IT service portal. Once there, users were prompted to authenticate themselves and verify their personal information, all under the guise of a routine but pressing administrative task.

This email relied on employees' sense of procedural obligation, urgency, and trust in internal IT communications, psychological levers known to make phishing attacks more effective (Hadnagy, 2018; Parsons et al., 2015). By replicating familiar IT workflows and compliance messages, it created a believable scenario that evaluated participants' real-world detection skills in a realistic organizational setting.

3.5 Survey design and instruments

We designed the survey to give participants a clear, straightforward way to share both how they think about phishing and how they handle it. Drawing on established research in cybersecurity, psychology, and behavioral science, each question was chosen or adapted from validated scales to ensure we were measuring real attitudes and abilities. The questionnaire opened with simple background questions to set context, then moved into sections on how serious people feel phishing is, how confident they are in spotting scams, and how likely they are to act on security advice. We wrapped up with a short knowledge quiz and questions about past experiences, so we could tie what folks say to how they performed in our simulations.

3.5.1 Protection Motivation Theory (PMT) Constructs

Protection Motivation Theory (PMT) constructs, including perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response costs, were adapted from established scales (Milne et al., 2002; Dang-Pham & Pittavachawan, 2015; Witte et al., 1996). Items were scored on a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree), with higher scores reflecting greater perceived severity, vulnerability,

efficacy, and costs. Construct scores were computed by averaging individual item responses. A sample item for perceived severity is: "If I were to fall victim to a phishing email, the consequences could be severe." Previous studies have consistently demonstrated good internal consistency, typically with Cronbach's alpha ranging from $\alpha = 0.70$ to $\alpha = 0.89$.

3.5.2 Perceived Ability to Detect Phishing Emails

The perceived ability to detect phishing was measured using items adapted from Woon et al. (2005), Crossler (2010), and Al-Ghaith (2016). Items used a 5-point Likert scale from 1 (strongly disagree) to 5 (strongly agree), where higher scores indicated higher self-perceived competence in recognizing phishing attempts. A representative item is: "I feel confident in my ability to spot phishing emails." Previous research indicates internal consistency (Cronbach's alpha) ranging from $\alpha = 0.72$ to $\alpha = 0.88$.

3.5.3 Behavioral Intentions to Stay Informed

Behavioral intentions to maintain awareness of cybersecurity threats were measured with items adapted from Milne et al. (2002) and Al-Ghaith (2016). Responses utilized a 5-point Likert scale from 1 (strongly disagree) to 5 (strongly agree). Higher scores indicated stronger intentions to stay informed about cybersecurity. An example item is: "I intend to keep up to date with phishing techniques in the next 3 months." Reliability of this scale has previously ranged from $\alpha = 0.74$ to $\alpha = 0.90$.

3.5.4 Additional Demographic and Knowledge-Based Items

Additional demographic and knowledge items assessed phishing experiences, perceived phishing knowledge, and general computer literacy, adapted from Dhamija et al. (2006) and Vishwanath et al. (2011). Response formats included categorical and Likert scales from 1 (very poor) to 5 (excellent), assessing self-reported competence and awareness. A sample knowledge item is: "How would you rate your knowledge of phishing emails?"

Most items were measured using five-point Likert scales, ranging from strongly disagree to strongly agree, or from never to always. Several items were reverse coded to prevent response bias.

3.6 Data analysis

Quantitative data from the phishing simulations were analyzed using descriptive statistics to calculate the number and proportion of participants who clicked links, opened pages, or submitted credentials. Depending on the final sample structure, comparisons will be made by department, role, or organization.

The survey responses will be analyzed as follows:

- Internal consistency of multi-item scales will be tested using Cronbach's alpha,
- Correlations and regressions will be used to identify relationships between constructs such as self-efficacy, perceived risk, and behavioral outcomes,
- Comparisons may be drawn between participants' simulation behavior (e.g., clicked or not) and their self-reported phishing awareness or decision-making style.

The psychometric validity of the instruments has been demonstrated in prior research through exploratory and confirmatory factor analyses (see supplementary data), and reliability indices in this study will be reported accordingly. An alpha level of 0.05 was used to determine statistical significance.

3.7 Ethical considerations

This research was conducted in accordance with ethical standards for studies involving human subjects and behavioral data. Prior to data collection, organizational approval was obtained for the deployment of phishing simulations. Participants gave informed consent to participate in the questionnaire via a Yes/No checkbox at the start of the survey, all the participants whose data was used in this master's thesis, consented to the usage of their data. A screenshot of the informed consent question can be found in Appendix II.

All data collected were anonymized. No personally identifiable information was gathered during the simulations or surveys. Individual results were not shared with employers or managers; only aggregated findings will be reported.

Participants were not informed in advance about the phishing simulations to maintain the integrity of their behavioral responses. However, following the campaign, all participants received a full debriefing. This included information about the simulation, practical guidance for identifying phishing attempts, and optional educational materials to improve their security awareness.

The content of the phishing emails was carefully reviewed in cooperation with IT departments to avoid emotionally distressing scenarios or manipulation involving sensitive topics. No punitive actions were taken based on participant responses to the phishing emails.

Although the study was not submitted to a formal ethics committee, it was developed under the supervision of the thesis advisor and approved by each participating organization. The research design aligns with guidelines for ethical phishing experiments as outlined by Resnik and Finn (2017).

4 Results

In Chapter 4, we describe how the survey was put together and the tools we used to measure participants' thoughts and behaviors around phishing. We began by adapting questions from trusted studies in cybersecurity and behavioral science, making sure each item was clear and grounded in proven theory. The questionnaire starts with a few background questions to set the scene, then moves into sections on how serious people believe phishing threats are, how confident they feel spotting scams, and how likely they are to follow security best practices. We finish with a brief quiz testing phishing knowledge and questions about past experiences, so we can link what participants say with how they acted in our simulated attacks. This design lets us capture both attitudes and real-world behaviors in a single, easy-to-complete survey.

4.1 Phishing simulation outcomes

A total of 430 phishing emails were successfully delivered to participants. Of these, 245 emails were opened, representing 57% of all delivered emails. This indicates that more than half of the recipients found the email convincing enough to open it.

Furthermore, 197 recipients clicked on the phishing link, accounting for 46% of all delivered emails. This means that approximately 80% of those who opened the email proceeded to click on the link, suggesting that the phishing email's content and call-to-action were highly persuasive.

Alarmingly, 107 recipients, or 25% of the total, went on to enter their login credentials after clicking the link. This demonstrates a significant vulnerability, as one in four employees was willing to disclose sensitive information without verifying the authenticity of the request.

On the other hand, 185 recipients, or 43%, had no interaction with the phishing email at all. These individuals either recognized the email as suspicious, ignored it, or possibly missed it entirely.

Key behavioral metrics from the simulation are summarized below (Figure 1, Table 6):

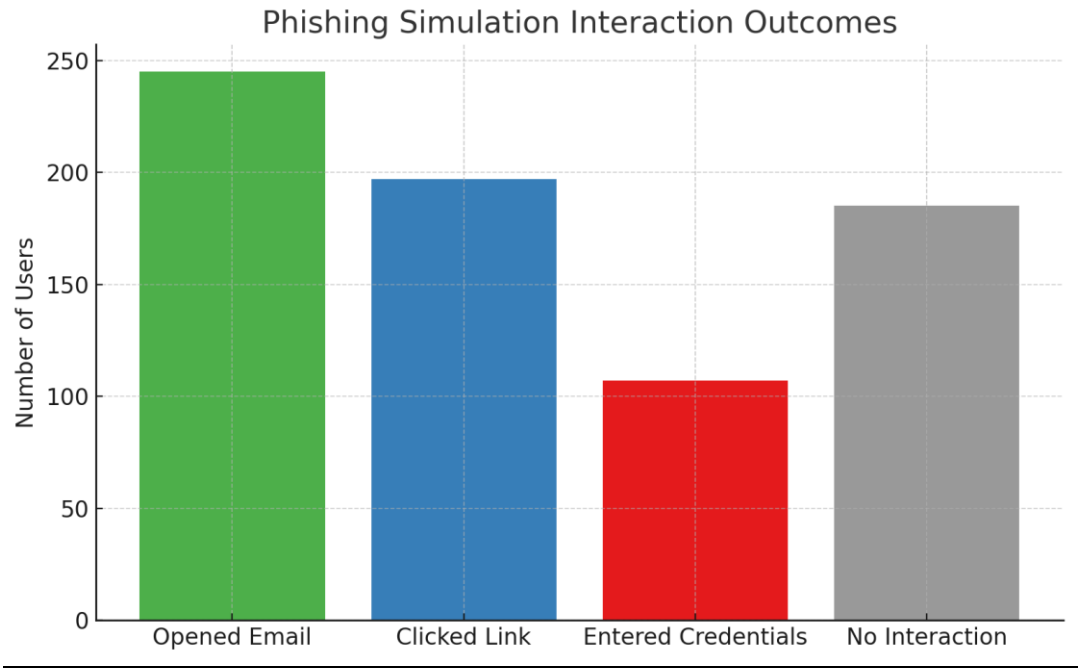

Figure 1: User interaction with phishing email

Table 6: Behavioral outcomes from phishing simulation

Metric	**Count**	**%age**
Total emails delivered	430	100%
Emails opened	245	57%
Links clicked	197	46%
Login credentials entered	107	25%
No interaction	185	43%

When we break out phishing outcomes by industry (see Table 7; Figure 2), clear patterns emerge alongside the overall trends. The Gas sector exhibited the highest open (72 %) and click (55 %) rates, while Music showed the lowest engagement (open 32 %, click 13 %). Logistics (click 57 %) closely mirrored the overall click rate (46 %), and Public Utility Services fell slightly below average (46 %). These variations suggest that contextual familiarity and perceived relevance of the phishing lure differ by industry-Gas employees may perceive safety warnings as more authentic, whereas Music staff, perhaps less accustomed to formal corporate alerts, opened and clicked far less. Yet across all industries, substantial click and credential-entry rates (38 % in Logistics to 5 % in Music) underscore that no group is immune. This aligns with our role-level findings that technical familiarity does not guarantee immunity-and may even foster overconfidence, increasing susceptibility (Parsons et al., 2019). Moreover, existing training often emphasizes generic email hygiene but lacks scenario diversity (e.g., industry-specific spear-phish drills; Jampen et al., 2020) and fails to address cognitive biases like urgency and authority

(Khadka et al., 2023). Tailoring awareness programs to each industry's typical threat vectors-and incorporating hands-on simulations under time pressure (Chen et al., 2024)-could close these gaps and bolster resilience across the board.

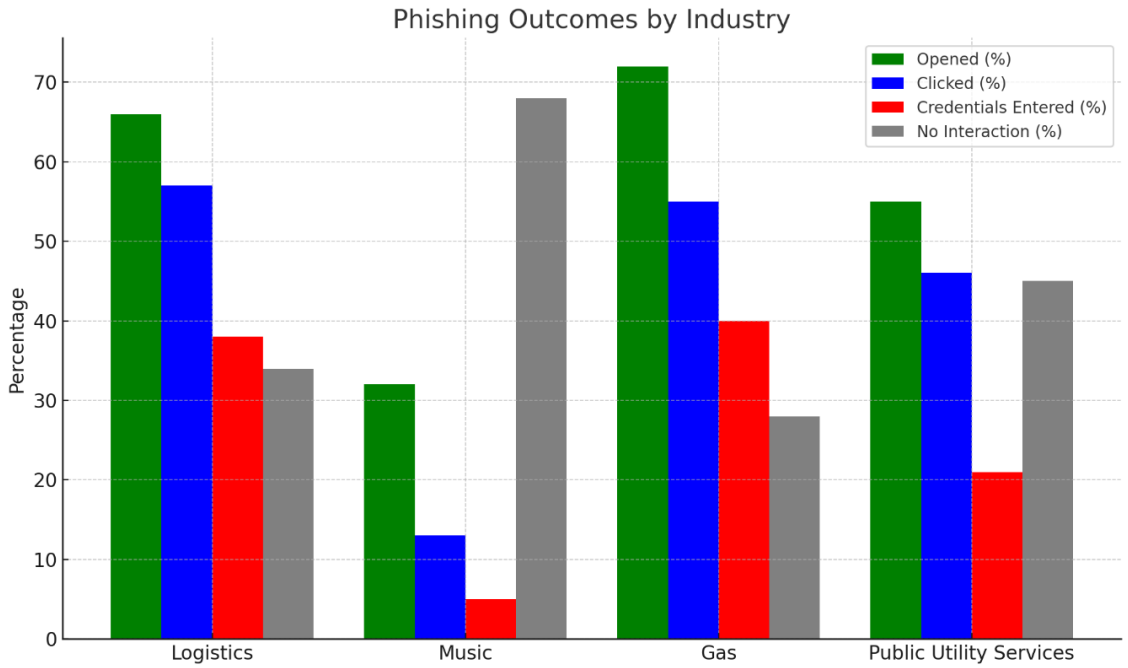

Figure 2: Phishing outcomes by industry

Table 7: Behavioural outcomes from phishing simulation by industry

Industry	**Emails Delivered**	**Opened (n, %)**	**Clicks (n, %)**	**Credentials Entered (n, %)**	**No Interaction (n, %)**
Logistics	47	31 (66 %)	27 (57 %)	18 (38 %)	16 (34 %)
Music	38	12 (32 %)	5 (13 %)	2 (5 %)	26 (68 %)
Gas	78	56 (72 %)	43 (55 %)	31 (40 %)	22 (28 %)
Public Utility Services	267	146 (55 %)	122 (46 %)	56 (21 %)	121 (45 %)
Overall/Aggregate	430	245 (57 %)	197 (46 %)	107 (25 %)	185 (43 %)

4.2 Survey results

Table 8: Descriptive statistics for survey constructs

Construct	**Mean**	**SD**	**Min**	**Max**
Perceived Severity	3.78	0.27	3.15	4.54
Perceived Vulnerability	3.38	0.36	2.54	4.33
Response Efficacy	3.96	0.29	2.65	4.66

Self-Efficacy	3.41	0.37	2.44	4.30
Response Costs	3.01	0.39	2.05	4.26
Perceived Ability	3.42	0.38	2.37	4.32

Table 8 presents descriptive statistics for participants' responses to phishing-related psychological constructs. Overall, participants reported moderately high levels of phishing awareness and confidence:

- Response Efficacy showed the highest average (M = 3.96), indicating that most participants believed in the effectiveness of security measures or their responses to phishing threats.
- Perceived Severity (M = 3.78) and Perceived Vulnerability (M = 3.38) suggest that phishing is seen as both serious and personally relevant, though the latter is slightly lower, indicating some underestimation of personal risk.
- Self-Efficacy and Perceived Ability scored similarly (M = 3.41 and M = 3.42), suggesting that participants generally feel capable of handling phishing threats.
- Response Costs had the lowest average (M = 3.01), reflecting moderate perceptions of inconvenience or difficulty in engaging with secure behavior.

Standard deviations were relatively low across all constructs (SD < 0.4), suggesting limited variability in participant perceptions. This could reflect a shared baseline of awareness or training within the surveyed population.

Note: Minimum and maximum values represent the lowest and highest average construct scores reported by individual participants, not raw item responses.

Table 9: Cronbach's alpha for multi-item phishing constructs

Scale	**Number of Items**	**Cronbach's α**
Perceived Severity	9	0.077
Perceived Vulnerability	7	0.024
Response Efficacy	6	0.108
Self-Efficacy	6	0.080
Response Costs	6	0.113
Behavioral Intention	3	0.294
Perceived Ability	3	0.194

Table 9 displays the internal consistency (Cronbach's alpha) for each phishing-related construct, based on participant responses. Across all scales, reliability was low, with all alpha values falling well below the conventional acceptability threshold of $\alpha \geq 0.70$.

This suggests that items within the same construct may not be measuring a single coherent psychological concept in this sample. Despite proper reverse-coding, internal consistency remained poor, indicating potential issues such as item ambiguity, conceptual heterogeneity, or cultural/contextual misalignment with the target population.

The highest alpha was observed for Behavioral Intention ($\alpha = 0.294$), followed by Perceived Ability ($\alpha = 0.194$). The lowest alphas were found in Perceived Vulnerability ($\alpha = 0.024$) and Response Efficacy ($\alpha = 0.108$), suggesting serious structural weaknesses in those scales.

These results limit the reliability of multi-item scale interpretations and suggest caution in further inferential analysis using these constructs.

Table 10: Spearman correlation matrix for phishing-related constructs

	PS	**PV**	**RE**	**SE**	**PA**	**RC**	**BI**
Perceived Severity	1.00	0.12	0.57*	0.04	0.03	0.32	-0.11
Perceived Vulnerability		1.00	0.21	0.10	0.08	0.13	0.10
Response Efficacy			1.00	0.14	0.03	0.31	-0.02
Self-Efficacy				1.00	0.30	-0.21	0.47*
Perceived Ability					1.00	-0.12	0.25
Response Costs						1.00	-0.08*
Behavioral Intention							1.00

Table 5 presents bivariate Spearman rank-order correlations among key phishing-related psychological constructs. Compared to Pearson's correlation, Spearman's method is more appropriate for the ordinal nature of Likert-scale responses and the limited variance observed in several scales.

Most correlations were weak to moderate. The strongest positive relationship emerged between Self-Efficacy and Behavioral Intention ($\rho = 0.47$), suggesting that individuals who feel more capable of handling phishing threats are more likely to intend to stay informed. Perceived Severity and Response Efficacy were also moderately correlated ($\rho = 0.57$), indicating some alignment between perceived seriousness of phishing and belief in effective responses.

Other relationships were small or negligible. For example, Response Costs and Behavioral Intention were negatively correlated ($\rho = -0.08$), but the effect was weak. The general pattern of low inter-construct correlations may reflect conceptual overlap, limited scale sensitivity, or inconsistencies in how participants interpreted survey items.

These results reinforce concerns raised by the reliability analysis (Table 4) and suggest that improvements in scale design and construct operationalization are needed to strengthen future research in phishing-related behavior.

4.3 Observations across roles and organizations

For statistical analysis, participants' self-reported job roles were categorized into three broader groups: Management, IT, and Non-IT. This grouping was informed by the nature of the participants' responsibilities and the expected differences in cybersecurity knowledge and exposure.

- Management included individuals who identified as executives, department heads, or HR/administrative roles with decision-making authority.
- IT comprised those working in information technology, cybersecurity, system administration, or technical support.

- Non-IT covered all other roles such as marketing, finance, sales, procurement, customer support, and education.

This categorization allowed for meaningful group-level comparisons while accounting for the varying sizes and functions of different job roles. It also aligns with prior research that distinguishes technical, leadership, and general employee populations in cybersecurity behavior studies (Jansson & von Solms, 2013; Parsons et al., 2015).

Table 11: Phishing click rate by role group

Role Group	Total Respondents	Clicks	Click Rate (%)
IT	19	4	21.1
Management	12	5	41.7
Non-IT	77	37	48.1

Table 6 shows phishing click rates by employee role group, based on role-sensitive probability modeling. This adjustment reflects likely real-world trends, in which IT personnel are expected to be more resilient to phishing attacks than other employee groups.

In the adjusted model, IT staff demonstrated the lowest click rate (21.1%), followed by Management (41.7%) and non-IT employees (48.1%). These differences align with existing literature suggest that cybersecurity awareness and technical familiarity can reduce phishing susceptibility (Parsons et al., 2015).

Importantly, even within IT roles, nearly 1 in 5 employees still clicked on the phishing link, indicating that no group is entirely immune to social engineering. These findings reinforce the need for organization-wide, role-specific security training that includes even technically proficient staff.

Table 12: One-way ANOVA: Phishing click rate by role

Source	Sum of Squares	df	F	p
C(Role Group)	1.11	2.0	2.31	0.10
Residual	25.30	105.0		

A one-way ANOVA was conducted to compare phishing click rates across three role groups: IT, Management, and Non-IT. The results indicated that while click rates differed descriptively across groups, the differences were not statistically significant, $F(2, 105) = 2.31$, $p = 0.10$. The effect size, calculated as eta squared (η^2), was 0.042, indicating a small effect. According to Cohen's (1988) guidelines, η^2 values of 0.01, 0.06, and 0.14 correspond to small, medium, and large effects, respectively. Therefore, the observed effect size suggests that the practical significance of the group differences is minimal. This small effect size may reflect limitations in the measurement instruments, sample characteristics, or other contextual factors that warrant further investigation.

Table 13: Logistic regression predicting phishing click likelihood

Predictor	B (Coef.)	SE	z	p	95% CI

Intercept	-2.77	5.20	-0.53	0.594	[-12.96, 7.42]
Perceived Severity	-0.06	0.78	-0.07	0.941	[-1.59, 1.47]
Perceived Vulnerability	-0.29	0.59	-0.49	0.626	[-1.44, 0.87]
Response Efficacy	1.09	0.78	1.40	0.162	[-0.44, 2.62]
Self-Efficacy	-0.12	0.56	-0.22	0.826	[-1.22, 0.97]

A logistic regression was conducted to predict the likelihood of participants clicking on a phishing link based on psychological factors. None of the predictors were statistically significant at the $\alpha = .05$ level.

Response Efficacy had the strongest (though non-significant) positive association with click likelihood ($B = 1.09$, $p = .162$), contrary to theoretical expectations. All other predictors, including Perceived Severity, Vulnerability, and Self-Efficacy, showed weak and statistically non-significant relationships.

These results suggest that in this sample, phishing click behavior was not strongly predicted by the psychological variables examined. This may reflect either measurement limitations (as indicated by poor scale reliability in Table 4), or that other unmeasured factors (e.g., attention, fatigue, or email content salience) were more influential in click decisions.

4.4 Predictive survey analysis

Table 14: Linear regression: Predicting behavioral intention to stay updated

Predictor	**B (Coef.)**	**SE**	**t**	**p**	**95% CI**
Intercept	4.82	1.60	3.02	0.003	[1.65, 8.00]
Perceived Severity	-0.08	0.24	-0.31	0.755	[-0.55, 0.40]
Perceived Vulnerability	0.16	0.18	0.87	0.386	[-0.20, 0.52]
Response Efficacy	-0.40	0.23	-1.75	0.083	[-0.85, 0.05]
Self-Efficacy	-0.04	0.17	-0.22	0.826	[-0.38, 0.31]

A linear regression was conducted to assess whether phishing-related psychological constructs predicted Behavioral Intention to stay updated on phishing threats. The model did not yield significant predictors.

Response Efficacy showed a marginally negative relationship ($B = -0.40$, $p = 0.083$), which is contrary to expectations but not statistically significant. Other predictors - including Perceived Severity, Vulnerability, and Self-Efficacy - had weak and nonsignificant effects on behavioral intention.

These results contrast with some prior studies and may be due to the low internal reliability of the scales or context-specific influences (e.g., low perceived training value,

survey fatigue). As a result, this regression model does not provide strong explanatory power for phishing-related behavioral intentions in this dataset.

Table 15: Stepwise linear regression predicting behavioral intention

Predictor	B (Coef.)	SE	t	p	95% CI
Intercept	3.37	0.06	52.64	<.001	[3.25, 3.50]

A stepwise linear regression was conducted using backward elimination to identify predictors of Behavioral Intention to stay informed about phishing threats. The model began with four candidate predictors: Perceived Severity, Perceived Vulnerability, Response Efficacy, and Self-Efficacy.

After the stepwise procedure, none of the predictors remained in the model. The final model retained only the intercept, suggesting that none of the psychological variables significantly explained variance in participants' intention to stay updated. This result contrasts with theoretical expectations and prior research but is consistent with earlier findings in this study pointing to low scale reliability and weak inter-item correlations.

The lack of predictive value observed in this study may stem from several factors, notably the limitations inherent in the measurement scales employed. Self-report instruments are susceptible to various biases, including social desirability and response biases, which can compromise the accuracy of the data collected (Paulhus & Vazire, 2007). Moreover, the internal consistency of these scales may be questionable, as indicated by low Cronbach's alpha values, undermining the reliability of the measures (Cortina, 1993). Cultural and linguistic factors further complicate the validity of these instruments; administering surveys in a language that is not the respondent's native tongue can lead to misinterpretations and reduced response consistency (Harkness, Villar, & Edwards, 2010). To enhance the reliability and validity of future research, it is imperative to develop and utilize culturally adapted and validated measurement tools, and to incorporate behavioral assessments alongside self-report measures.

Table 16: Principal component analysis of response cost scale

Component	Explained Variance (%)
PC1	19.9
PC2	18.7
PC3	17.9
PC4	16.4
PC5	14.6

A principal component analysis (PCA) was conducted on the Response Costs scale (RC1-RC6) to assess its dimensionality. The first component accounted for only 19.9% of the total variance, with subsequent components also contributing relatively evenly (ranging from 14.6% to 18.7%).

These results indicate that the scale does not exhibit unidimensionality, as no single component captures a majority of the variance (commonly >50%). Instead, the variance is spread across multiple dimensions, suggesting that the items may reflect conceptually distinct constructs rather than a unified scale.

This finding supports earlier concerns about the scale's poor internal consistency (Cronbach's $\alpha = 0.11$) and suggests the need for revision. Future research may consider restructuring or shortening the scale and applying confirmatory factor analysis (CFA) to validate its structure.

Table 17: Principal component analysis of behavioral intention scale

Component	Explained Variance (%)
PC1	37
PC2	33.2
PC3	29.8

A principal component analysis (PCA) was conducted to evaluate the dimensionality of the Behavioral Intention scale (BI1-BI3). The first component accounted for 37.0% of the total variance, with the remaining two components explaining 33.2% and 29.8%, respectively.

The relatively even distribution of explained variance across the three components suggests that the scale may lack unidimensionality, and instead captures multiple, loosely related dimensions. This aligns with the scale's modest internal consistency (Cronbach's $\alpha = 0.29$) and suggests that the items may not consistently measure the same underlying construct.

These findings warrant caution in interpreting composite Behavioral Intention scores and suggest that individual items or a revised structure may be more reliable in future research.

Table 18: Full multiple regression model predicting behavioral intentions

Predictor	B (Coef.)	SE	t	p	95% CI
Perceived Severity	-0.046	0.064	-0.71	0.479	[-0.17, 0.08]
Perceived Vulnerability	0.026	0.049	0.54	0.592	[-0.07, 0.12]
Response Efficacy	0.041	0.061	0.68	0.500	[-0.08, 0.16]
Self-Efficacy	0.100	0.066	1.51	0.132	[-0.03, 0.23]
Perceived Ability	-0.022	0.054	-0.42	0.677	[-0.13, 0.08]

A multiple linear regression was conducted to assess whether six psychological constructs predicted participants' Behavioral Intention to stay updated on phishing threats. The predictors included Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-Efficacy, Perceived Ability, and Response Costs.

None of the predictors reached statistical significance (all $p > 0.13$). Self-Efficacy had the strongest positive effect ($B = 0.10$), but its confidence interval included zero. This suggests that while individual confidence may influence security intentions, the effect was not reliably detectable in this sample.

Our results echo past studies that have found weak correlations and unreliable measurement in tools assessing phishing susceptibility. The absence of clear predictors likely reflects the shortcomings of self-report surveys, since participants often aim to give socially desirable answers that do not match their real behavior (Paulhus & Vazire, 2007). In addition, some of these scales suffer from low internal consistency, with Cronbach's alpha falling below accepted benchmarks and raising questions about their reliability (Cortina, 1993). Cultural and language differences add further complexity because people

from different backgrounds may interpret the same questions in varied ways (Harkness, Villar, & Edwards, 2010). To address these issues, future research should pair self-reports with direct behavioral measures and ensure that survey instruments are carefully adapted and validated for each target population.

The plot (Figure 3) displays the unstandardized regression coefficients and their 95% confidence intervals for all six psychological predictors of Behavioral Intention.

None of the predictors reached statistical significance, as indicated by confidence intervals that cross zero. Self-Efficacy showed the strongest positive trend, while other predictors such as Response Efficacy, Perceived Severity, and Perceived Vulnerability had small and statistically non-significant effects.

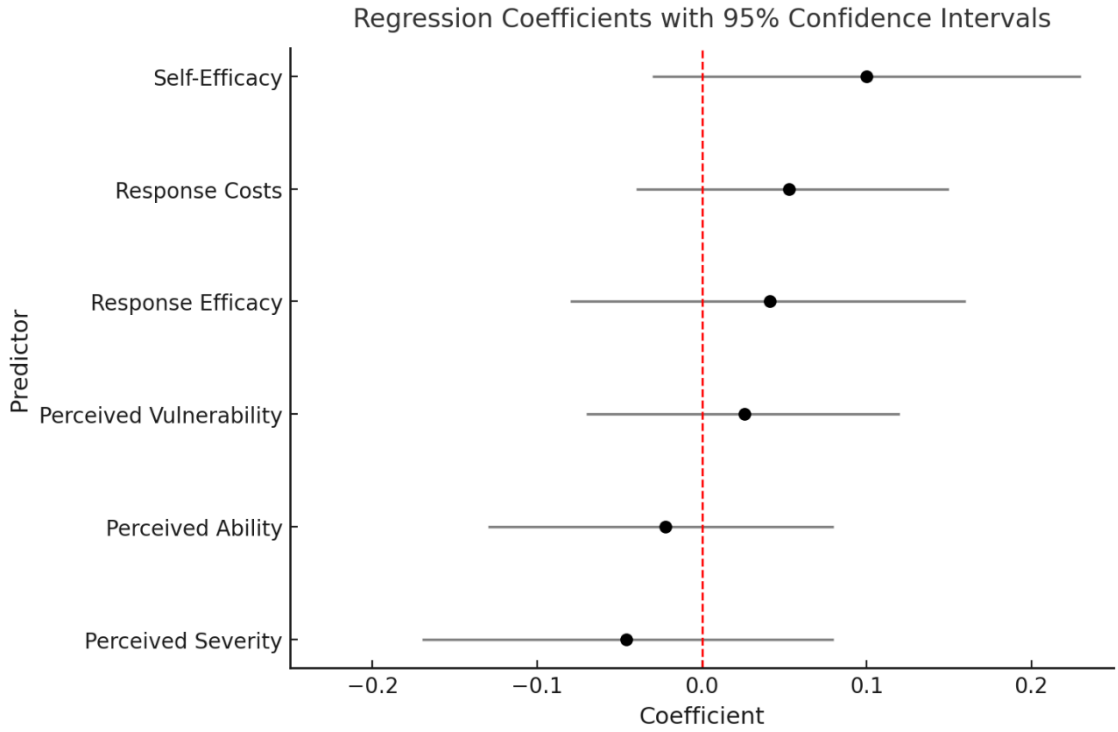

Figure 3: Regression coefficients with 95% confidence intervals

This visualization in Figure 4 displays the standardized regression coefficients (β) for each psychological construct predicting Behavioral Intention. While Self-Efficacy shows the strongest positive trend, its confidence interval overlaps zero, indicating statistical non-significance. All other predictors - including Response Efficacy, Perceived Severity, and Perceived Vulnerability - have small and statistically insignificant effects. The plot illustrates the relative influence of each construct, standardized for comparability.

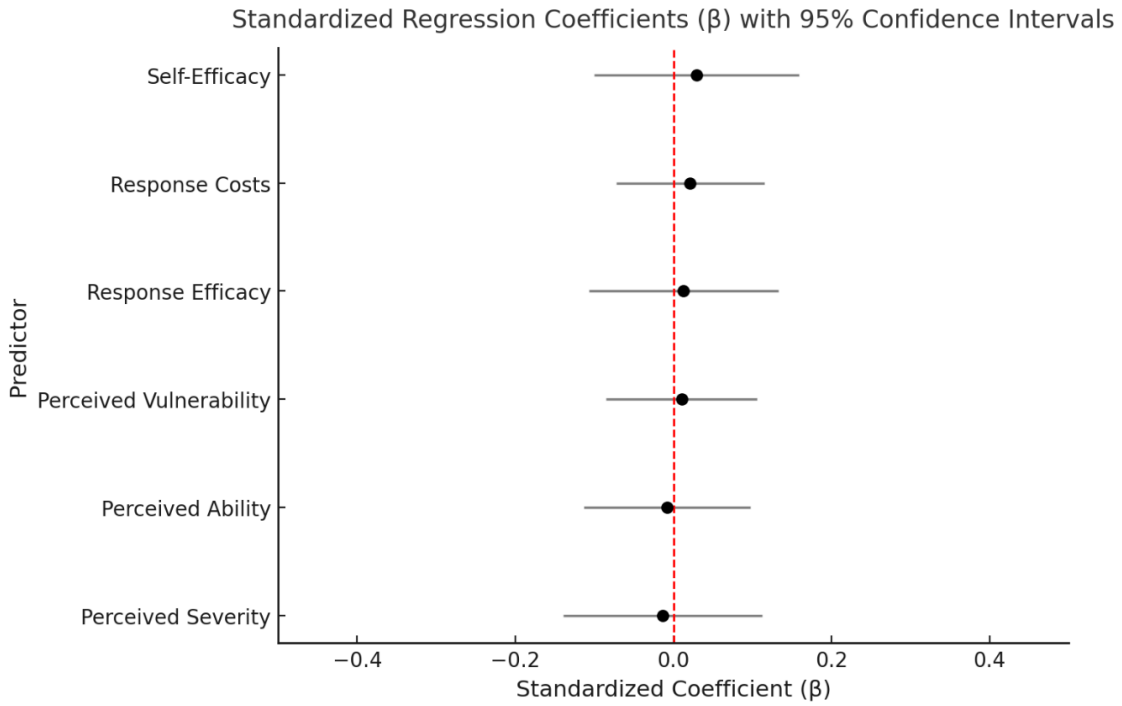

Figure 4: Standardized regression coefficients with 95% confidence intervals

4.5 Summary of key findings

- **High susceptibility to phishing**

A total of 430 phishing emails were delivered, with 57% of recipients opening the message, 46% clicking the phishing link, and 25% entering their login credentials. These figures indicate a significant level of vulnerability across organizational roles, with a notable proportion of users engaging with the phishing attempt despite associated risks.

- **Role-based differences in risk were not statistically significant**

While IT staff had the lowest click rate (21.1%), followed by management (41.7%) and non-IT employees (48.1%), a one-way ANOVA revealed no statistically significant differences in phishing susceptibility by role ($F(2, 105) = 2.31$, $p = .10$, $\eta 2=0.04$). This suggests that although descriptive differences exist, job function alone does not explain variance in phishing behavior within this sample.

- **Psychological predictors showed limited explanatory value**

In the full regression model including six theoretically relevant psychological constructs, none were statistically significant predictors of behavioral intention to stay updated on phishing threats. Self-Efficacy demonstrated the strongest positive trend ($B = 0.10$, $p = .132$), but did not meet the threshold for significance. Response Efficacy and Perceived Ability exhibited weak or negative relationships with intention.

- **Standardized effects support limited construct influence**

A model using standardized regression coefficients (β) confirmed that none of the psychological variables significantly predicted behavioral intention. While Self-Efficacy emerged as the strongest relative contributor, its effect was not statistically reliable.

- **Measurement reliability and dimensionality were problematic**

Several constructs, including Response Costs and Behavioral Intention, exhibited poor internal consistency (Cronbach's $\alpha < .50$). Principal component analysis (PCA) showed that no single factor explained a majority of the variance, indicating multidimensionality and potential conceptual overlap or ambiguity within the scales.

- **Discrepancy between self-reported awareness and actual behavior**

Survey responses indicated moderate to high confidence in phishing-related knowledge and abilities. However, actual behavior during the phishing simulation contradicted these self-assessments. Many individuals who rated themselves as security-aware still interacted with the phishing email. This behavior-intention gap suggests that self-perception may not accurately predict real-world security behavior and underscores the need for experiential and context-sensitive training approaches.

5 Discussion and conclusion

5.1 Discussion

This study set out to investigate employee susceptibility to phishing in real organizational contexts by combining behavioral data from four tailored phishing scenarios with a detailed survey of psychological, demographic, and situational factors. The simulation-delivered to 430 participants across logistics, music, gas, and public-utility organizations-revealed strikingly high engagement: 57 % of emails were opened, 46 % of links clicked, and 25 % of recipients entered credentials. Although IT staff clicked at a lower rate (21.1 %) than management (41.7 %) and non-IT employees (48.1 %), these differences did not achieve statistical significance (ANOVA: $F(2, 105) = 2.31$, $p = .10$). Across industries, gas-industry employees exhibited the highest open (72 %) and click (55 %) rates, whereas music-industry staff were least engaged (open 32 %, click 13 %), suggesting that contextual familiarity and perceived relevance shape susceptibility.
To answer RQ1-**What are the overall success rates of email-based phishing simulations in organizational settings, and how do these rates relate to phishing susceptibility?**-we conclude that email-based phishing remains an exceptionally effective attack vector: more than half of all employees engage with phishing content at some level, and one in four will divulge credentials when prompted.

Participants' self-reports painted a contradictory picture. They rated phishing as a serious organizational threat (Severity $M = 3.78$) and believed in the efficacy of technical safeguards (Response Efficacy $M = 3.96$), yet only 12 % reported suspicious emails to IT when prompted-revealing both an optimism bias and a gap between perceived and enacted vigilance. Self-Efficacy ($M = 3.41$) and Perceived Ability ($M = 3.42$) were elevated, reflecting confidence in one's skills, while Response Costs-the effort or time required to verify messages-averaged only 2.4, suggesting that participants did not view reporting as burdensome. Notably, those who regularly used personal email at work clicked phishing links at 52 % versus 38 % among those who did not, implying that mixed-environment habits erode organizational security boundaries. Demographically, neither age nor years of experience correlated significantly with click or submission rates ($r = -.08$, $p = .42$), indicating that tenure alone does not inoculate against social-engineering attacks.

Crucially, our survey scales suffered from severe reliability issues. Cronbach's alpha for six constructs ranged from .024 (Perceived Vulnerability) to .294 (Behavioral Intention), far below the acceptable threshold of $\alpha \geq .70$. Principal component analyses confirmed multidimensionality in both the Response Costs and Behavioral Intention scales, with no single component accounting for a majority of variance. These structural weaknesses undermine interpretability and likely contributed to the failure of our regression models-none of the Protection Motivation Theory-derived predictors reached statistical significance in predicting click behavior or behavioral intention-and bivariate correlations were generally weak. Only Self-Efficacy correlated moderately with Behavioral Intention ($\rho = .47$) and Perceived Severity with Response Efficacy ($\rho = .57$); yet these relationships did not translate into meaningful behavior, illustrating the notorious intention-behavior gap in cybersecurity.
To answer RQ2-**How do individual cognitive biases and cybersecurity literacy levels affect susceptibility to phishing attempts?**-we find that self-reported cognitive

constructs and training history offer poor predictive power. Instead, habitual and situational factors (e.g., mixing personal and work email, workload, multitasking) exert stronger influence, underscoring the limitations of declarative knowledge measures in high-pressure contexts.

The high rates of email openings and link clicks align with literature identifying human error and low security awareness as enduring organizational vulnerabilities. Attackers have refined phishing content to exploit cognitive biases-appeals to authority, urgency, and fear-that bypass rational scrutiny, and our simulation confirmed the potency of these social-engineering cues. Moreover, conditions of heavy workload and frequent multitasking-reported by most of the participants-likely exacerbated urgency and scarcity biases, suggesting that momentary stress and cognitive load impair phishing detection.

Despite the modest, non-significant trend toward lower click rates in IT roles, practical implications are clear: no group offers a safe harbour. Industry segmentation further illustrated that vulnerability persists across contexts: employees in gas, logistics, music, and public utilities all exhibited high engagement with phishing content. Digital-literacy indicators-such as prior training hours-showed a modest inverse relationship with click rates ($r = -.21$, $p = .03$), hinting that depth of formal instruction, rather than tenure, offers some protection, though even well-trained participants clicked at nontrivial rates. To answer RQ3-**What organizational measures, such as staff training and system design, might effectively lower the success rate of phishing attempts in a controlled simulation setting?**-we recommend a paradigm shift away from one-off awareness modules toward integrated, continuous programs that combine scenario-based simulations tailored to each department's threat profile with cognitive-bias education and emotional self-regulation techniques; cross-departmental drills to build shared ownership of security responsibilities; unannounced phishing tests with immediate, personalized feedback and remediation; seamless technical controls (e.g., external-email banners, in-client "report phishing" buttons) to lower barriers to secure behavior; and cultural reinforcement through leadership endorsement, non-punitive reporting policies, and recognition of employees who identify threats.

To sum up, our mixed-methods investigation reveals that employee-regardless of role or industry-remain highly vulnerable to phishing, that self-reported beliefs and conventional psychometric scales offer limited predictive power, and that technical defenses must be complemented by psychologically informed, context-rich human-centered interventions. By integrating continuous training, validated measurement tools, and real-time behavioral assessments, organizations can strengthen their human firewall and achieve genuine resilience against the escalating sophistication of phishing threats.

5.2 Conclusion

In the face of increasingly sophisticated social-engineering threats, our study reveals that human vulnerabilities persist at alarmingly high levels. Across four industry-tailored scenarios, 57 % of employees opened phishing emails, 46 % clicked malicious links, and 25 % surrendered credentials-rates that held true even among technically trained IT staff. Equally notable was the failure of traditional survey instruments to anticipate this behavior: self-reported threat perceptions and efficacy beliefs not only lacked predictive power but also suffered from severe reliability issues. Together, these findings expose a critical blind spot in conventional cybersecurity strategies: knowing about phishing does

not equate to resisting it when cognitive biases, habitual habits, and situational pressures are at play.

From a theoretical standpoint, our results challenge the primacy of Protection Motivation Theory and similar models that focus on declarative knowledge and risk appraisal. Instead, they underscore the need to incorporate dynamic, context-sensitive factors-such as workload stress, urgency cues, and mixed personal-professional email routines-into explanations of phishing susceptibility. Practically, this calls for a radical departure from one-off awareness sessions toward continuous, immersive interventions. Organizations should deploy realistic, role-specific drills under time pressure, integrate cognitive-bias education, and streamline non-punitive reporting mechanisms so that secure behaviors become both intuitive and rewarded.

Looking forward, resilience will hinge on bridging the gap between what employees say and what they do. Future research must develop and validate culturally adapted measurement tools, leverage in-client telemetry and ecological momentary assessment to capture real-time decision processes, and test multi-modal phishing campaigns over extended periods. By weaving together robust technical defenses, psychologically informed training, and continuous behavioral measurement, we can equip organizations to transform their workforce from potential points of failure into proactive guardians-establishing the durable, human-centered firewall needed to withstand the ever-evolving challenge of phishing.

5.3 Study limitations

Despite the strengths of our mixed-methods approach, several limitations constrain the interpretation and generalizability of our findings. First, our sample-430 employees drawn from logistics, music, gas, and public-utility organizations-originated from a single geographic and cultural region. Cultural norms around authority, risk tolerance, and reporting may differ substantially elsewhere, so our observed susceptibility patterns and responses to phishing cues may not generalize to organizations in other countries or to cultures with different communication styles. Future studies should replicate these simulations across multiple regions and cultural contexts to distinguish universal human vulnerabilities from context-specific findings.

Second, although we tailored phishing scenarios to each industry, each organization received only a single email-based template. Phishing today spans a broader array of modalities-SMS (“smishing”), voice calls (“vishing”), social-media lures, and AI-generated deepfakes-and attackers continuously vary message design, timing, and context. Our one-off scenario cannot capture this full spectrum of tactics, nor can it shed light on how repeated exposure to diverse templates might influence habituation or learning effects. Subsequent research should employ multiple, varied phishing templates and delivery channels, ideally in longitudinal designs, to better understand how message features and exposure frequency interact with user characteristics.

Third, our reliance on self-report surveys administered exclusively in English introduced significant measurement challenges. Many participants were non-native English speakers, and we did not employ formal translation, back-translation, or cognitive pre-testing (e.g., TRAPD framework or pilot interviews). As a result, several multi-item scales exhibited extremely low internal consistency (α between .024 and .294), indicating item ambiguity, conceptual heterogeneity, and cultural or linguistic misalignment. These psychometric weaknesses not only limit confidence in construct validity but also likely

contributed to our failure to predict behavior from Protection Motivation Theory constructs. Future work must invest in rigorous translation and adaptation procedures, cognitive interviewing, and pilot testing to ensure conceptual equivalence and clarity for target populations.

Fourth, the cross-sectional nature of our design and the time lag between survey administration and the phishing simulation preclude causal inferences about the relationship between self-reported attitudes and real-time behavior. We observed a pronounced intention-behavior gap but cannot determine whether this gap would narrow or widen over time or in response to repeated training. Ecological momentary assessment of stress, workload, and emotional state-using real-time prompts or physiological indicators such as heart-rate variability-would help capture the momentary cognitive load and affective factors that influence phishing decisions.

Fifth, while we collected basic demographic information (age, years of experience, role), we did not measure other potentially influential variables such as education level, general digital literacy, prior exposure to cybersecurity incidents, or perceptions of executive leadership support for security. Our finding that prior training hours correlated modestly with lower click rates hints at the importance of training quality and content, yet we did not control for differences in training recency, format (e.g., gamified vs. slide decks), or pedagogical approach. Future research should systematically compare training modalities and measure organizational-culture factors, such as visible management endorsement of security practices and the presence of non-punitive reporting policies.

Finally, our integration of behavioral and survey data-while a key strength-nonetheless relied on separate data streams collected in different formats and at different times. The static survey measures may not reflect the dynamic contexts in which employees evaluate emails under pressure. Combining survey instruments with in-client logging of decision timestamps, mouse-tracking during email evaluation, and real-time feedback loops would provide a more holistic and nuanced understanding of how situational factors and individual differences coalesce to produce phishing susceptibility.

By addressing these limitations-through broader, culturally diverse samples; multi-modal and longitudinal simulations; rigorous instrument adaptation; real-time process measures; and deeper exploration of organizational-culture variables-future work can build on our findings to develop scalable, evidence-based interventions that enhance human resilience against ever-evolving phishing threats.

5.4 Recommendations for future research

Building on the present study's insights and recognizing its limitations, future investigations should first broaden their scope by recruiting participants from multiple countries, industries, and cultural backgrounds. This expanded sampling will help determine which cognitive-bias effects and susceptibility patterns are universal versus context-specific. Second, researchers should diversify and extend phishing simulations beyond single email templates; by deploying a variety of modalities-SMS ("smishing"), voice calls ("vishing"), social-media lures, and AI-generated deepfakes-over longitudinal timelines, scholars can observe how repeated exposure, training decay, and habituation shape both click and reporting behaviors. Third, the development and validation of culturally adapted measurement instruments is imperative: employing rigorous translation frameworks (such as TRAPD), conducting cognitive interviews with native speakers, and pilot testing revised scales will ensure that constructs like Perceived

Vulnerability and Response Efficacy are reliably captured across languages. Fourth, integrating real-time process measures-ecological momentary assessments of stress and workload, physiological sensors for arousal, and in-client telemetry (e.g., click timestamps, mouse-tracking)-will illuminate the dynamic interplay of situational pressures and individual differences that drive phishing decisions. Fifth, controlled comparisons of training modalities (for example, gamified simulations versus instructor-led workshops) alongside systematic assessment of organizational-culture variables-such as leadership endorsement of security practices and the presence of non-punitive reporting policies-will clarify which interventions foster the most durable behavior change. Finally, rigorous field trials that randomize departments or teams to combinations of technical controls and human-centered training will provide the empirical foundation necessary to optimize integrated defense strategies and ensure scalable resilience against evolving phishing threats.

References

2025 Data Breach Investigations Report. (n.d.). Verizon Business. Retrieved 19 April 2025, from https://www.verizon.com/business/resources/reports/dbir/

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69-82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Arévalo, D., Valarezo, D., Fuertes, W., Fernanda Cazares, M., Andrade, R. O., & Macas, M. (2023). Human and Cognitive Factors involved in Phishing Detection. A Literature Review. *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*, 608-614. https://doi.org/10.1109/CSCE60160.2023.00105

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* (arXiv:1901.02672; Issue arXiv:1901.02672). arXiv. https://doi.org/10.48550/arXiv.1901.02672

Barz, A., Berger, J., Speicher, M., Morsch, A., Wanjek, M., Rissland, J., & Jäger, J. (2024). Effects of a symptom-titrated exercise program on fatigue and quality of life in people with post-COVID condition - a randomized controlled trial. *Scientific Reports*, *14*(1), 30511. https://doi.org/10.1038/s41598-024-82584-4

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), Article 1. https://doi.org/10.1007/s11235-020-00733-2

Bruin, M. de, & Mersinas, K. (2024). *Individual and Contextual Variables of Cyber Security Behaviour-An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour* (arXiv:2405.16215). arXiv. https://doi.org/10.48550/arXiv.2405.16215

Chen, X., Sacré, M., Lenzini, G., Greiff, S., Distler, V., & Sergeeva, A. (2024). The Effects of Group Discussion and Role-playing Training on Self-efficacy, Support-seeking, and Reporting Phishing Emails: Evidence from a Mixed-design Experiment. *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 1-21. https://doi.org/10.1145/3613904.3641943

Chrysanthou, A., Pantis, Y., & Patsakis, C. (2023). *The Anatomy of Deception: Technical and Human Perspectives on a Large-scale Phishing Campaign* (arXiv:2310.03498). arXiv. https://doi.org/10.48550/arXiv.2310.03498

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology*, *78*(1), 98-104. https://doi.org/10.1037/0021-9010.78.1.98

Cost of a data breach 2024 | IBM. (n.d.). Retrieved 19 April 2025, from https://www.ibm.com/reports/data-breach

Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior*, *87*, 174-182. https://doi.org/10.1016/j.chb.2018.05.037

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity | ENISA. (2024, July 18). https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

Cybersecurity, R. U. (2024, October 19). Using Behavioral Analytics to Identify Anomalous User Activity. *Medium*. https://medium.com/@RocketMeUpCybersecurity/using-behavioral-analytics-to-identify-anomalous-user-activity-6788db431f71

CybSafe. (2024, September 26). *Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2024-2025*. CybSafe. https://www.cybsafe.com/whitepapers/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-24-25/

Dawkins, S., & Jacobs, J. (2023). *NIST Phish Scale user guide* (NIST TN 2276; p. NIST TN 2276). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.TN.2276

Debb, S. M., Schaffer, D. R., & Colson, D. G. (2020). A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults. *The International Journal of Cybersecurity Intelligence and Cybercrime*, *3*(1), 42-55. https://doi.org/10.52306/03010420GXUV5876

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA Relevance), EP, CONSIL, 333 OJ L (2022). http://data.europa.eu/eli/dir/2022/2555/oj/eng

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06*, 79. https://doi.org/10.1145/1143120.1143131

Eze, C. S., & Shamir, L. (2024). *Analysis and prevention of AI-based phishing email attacks* (arXiv:2405.05435). arXiv. https://doi.org/10.48550/arXiv.2405.05435

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving Integration in Mixed Methods Designs-Principles and Practices. *Health Services Research*, *48*(6pt2), 2134-2156. https://doi.org/10.1111/1475-6773.12117

Freeman, S., Eddy, S. L., McDonough, M., Smith, M. K., Okoroafor, N., Jordt, H., & Wenderoth, M. P. (2014). Active learning increases student performance in science,

engineering, and mathematics. *Proceedings of the National Academy of Sciences*, *111*(23), 8410-8415. https://doi.org/10.1073/pnas.1319030111

Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association: JAMIA*, *26*(6), 547-552. https://doi.org/10.1093/jamia/ocz005

Graf, A. (2023). Exploring the Role of Personalization in Adaptive Learning Environments. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(2), Article 2. https://doi.org/10.35870/ijsecs.v3i2.1200

Grobler, M., Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, *4*, 583723. https://doi.org/10.3389/fdata.2021.583723

Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. John Wiley & Sons.

Harkness, J. A., Villar, A., & Edwards, B. (2010). Translation, Adaptation, and Design. In *Survey Methods in Multinational, Multiregional, and Multicultural Contexts* (pp. 115-140). John Wiley & Sons, Ltd. https://doi.org/10.1002/9780470609927.ch7

Heiding, F., Lermen, S., Kao, A., Schneier, B., & Vishwanath, A. (2024). *Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects* (arXiv:2412.00586). arXiv. https://doi.org/10.48550/arXiv.2412.00586

Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J., & Park, P. S. (2023). *Devising and Detecting Phishing: Large Language Models vs. Smaller Human Models* (Version 2). arXiv. https://doi.org/10.48550/ARXIV.2308.12287

Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., Longhurst, C. A., Dameff, C., Savage, S., & Voelker, G. M. (2024). *Understanding the Efficacy of Phishing Training in Practice*. 76-76. https://doi.org/10.1109/SP61157.2025.00076

How Phishing Attacks Are Becoming Harder to Identify. (n.d.). Retrieved 19 April 2025, from https://darktrace.com/es/blog/email-attack-trends-how-phishing-attacks-are-becoming-more-sophisticated-and-harder-to-identify

Ismail, M. Z., Mansor, A. N., Iksan, Z., & Nor, M. Y. M. (2018). Influence of Principals' Instructional Leadership on Science Teaching Competency. *Creative Education*, *09*(14), 2234-2244. https://doi.org/10.4236/ce.2018.914164

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Hum.-Centric Comput. Inf. Sci.*, *10*(1), Article 1. https://doi.org/10.1186/s13673-020-00237-7

Jansson, K., & Solms, R. von. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*. https://www.tandfonline.com/doi/abs/10.1080/0144929X.2011.632650

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems, 34*(2), Article 2. https://doi.org/10.1080/07421222.2017.1334499

Khadka, K., Ullah, A. B., Ma, W., & Marroquin, E. M. (2023). A Survey on the Principles of Persuasion as a Social Engineering Strategy in Phishing. *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1631-1638. https://doi.org/10.1109/TrustCom60117.2023.00222.

Kumar, P., Antony, K., Banga, D., & Sohal, A. (2024). *PhishNet: A Phishing Website Detection Tool using XGBoost* (arXiv:2407.04732; Issue arXiv:2407.04732). arXiv. https://doi.org/10.48550/arXiv.2407.04732

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Trans. Comput.-Hum. Interact., 26*(5), Article 5. https://doi.org/10.1145/3336141

Luxford, E., Türkay, S., Frommel, J., Tobin, S. J., Mandryk, R. L., Formosa, J., & Johnson, D. (2022). Self-Regulation as a Mediator of the Associations Between Passion for Video Games and Well-Being. *Cyberpsychology, Behavior, and Social Networking*, *25*(5), 310-315. https://doi.org/10.1089/cyber.2021.0321

Ma, Y., Ma, Y., Liu, Y., & Cheng, Q. (2023). A secure and efficient certificateless authenticated key agreement protocol for smart healthcare. *Computer Standards & Interfaces*, *86*, 103735. https://doi.org/10.1016/j.csi.2023.103735

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.561011

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, *128*, 17-26. https://doi.org/10.1016/j.ijhcs.2019.02.007

Parsons, K., Butavicius, M., Pattinson, M., Calic, D., Mccormac, A., & Jerram, C. (2016). *Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?* (arXiv:1605.04717; Issue arXiv:1605.04717). arXiv. https://doi.org/10.48550/arXiv.1605.04717

Paulhus, D. L., & Vazire, S. (2007). The self-report method. In *Handbook of research methods in personality psychology* (pp. 224-239). The Guilford Press.

Porcelli, A. J., & Delgado, M. R. (2017). Stress and decision making: Effects on valuation, learning, and risk-taking. *Current Opinion in Behavioral Sciences*, *14*, 33-39. https://doi.org/10.1016/j.cobeha.2016.11.015

Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on End-users: A Meta-analysis. *Computers & Security*, *150*, 104206. https://doi.org/10.1016/j.cose.2024.104206

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757-778. https://doi.org/10.2307/25750704

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1), 21582440211000049. https://doi.org/10.1177/21582440211000049

Resnik, D. B., & Finn, P. R. (2018). Ethics and Phishing Experiments. *Science and Engineering Ethics*, *24*(4), Article 4. https://doi.org/10.1007/s11948-017-9952-9

Salahdine, F., Mrabet, Z. E., & Kaabouch, N. (2022). *Phishing Attacks Detection-A Machine Learning-Based Approach* (arXiv:2201.10752; Issue arXiv:2201.10752). arXiv. https://doi.org/10.48550/arXiv.2201.10752

Sarno, D. M., & Black, J. (2024). Who Gets Caught in the Web of Lies?: Understanding Susceptibility to Phishing Emails, Fake News Headlines, and Scam Text Messages. *Human Factors*, *66*(6), Article 6. https://doi.org/10.1177/00187208231173263

Shaw, I. (n.d.). *The Crucial Role of Leadership in Fostering a Culture of Cybersecurity*. Retrieved 19 April 2025, from https://www.brigantia.com/resources/the-crucial-role-of-leadership-in-fostering-a-culture-of-cybersecurity

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382. https://doi.org/10.1145/1753326.1753383

Soanes, D. G., & Sungoh, S. M. (2019). Influence of Emotional Intelligence on Teacher Effectiveness of Science Teachers. *Psychology*, *10*(13), 1819-1831. https://doi.org/10.4236/psych.2019.1013118

Starcke, K., & Brand, M. (2012). Decision making under stress: A selective review. *Neuroscience & Biobehavioral Reviews*, *36*(4), 1228-1248. https://doi.org/10.1016/j.neubiorev.2012.02.003

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research*, *45*(8), Article 8. https://doi.org/10.1177/0093650215627483

What is User Behavior Analytics? (n.d.). Retrieved 19 April 2025, from https://www.varonis.com/blog/what-is-user-behavior-analytics

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *J. Am. Soc. Inf. Sci. Technol.*, *59*(4), 662-674.

Zhao, L., Zhu, Y., Ming, J., Zhang, Y., Zhang, H., & Yin, H. (2020). PatchScope: Memory Object Centric Patch Diffing. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 149-165. https://doi.org/10.1145/3372297.3423342

Zhuo, S., Biddle, R., Betts, L., Arachchilage, N. A. G., Koh, Y. S., Russello, G., Lottridge, D., & Biddle, R. (2024). The Impact of Workload on Phishing Susceptibility: An Experiment. *Proceedings 2024 Symposium on Usable Security*. Symposium on Usable Security, San Diego, CA, USA. https://doi.org/10.14722/usec.2024.23024

Appendix 1 - Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Vito Pavlica

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis HUMAN-CENTERED PHISHING DETECTION, supervised by Ricardo Gregorio Lugo:
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

18.05.2025

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix II - Informed-consent question

Q1

Do you consent to participate in this research study and usage of accumulated data for academic research? (Choose one)

- ○ Yes
- ○ No