PeerJ Computer Science

A review of organization-oriented phishing research

Kholoud Althobaiti and Nawal Alsufyani

Department of Computer Science, Taif University, Taif, Saudi Arabia

ABSTRACT

The increased sophistication and frequency of phishing attacks that target organizations necessitate a comprehensive cyber security strategy to handle phishing attacks from several perspectives, such as the detection of phishing and testing of users' awareness. Through a systematic review of 163 research articles, we analyzed the organization-oriented phishing research to categorize current research and identify future opportunities. We find that a notable number of studies concentrate on phishing detection and awareness while other layers of protection are overlooked, such as the mitigation of phishing. In addition, we draw attention to shortcomings and challenges. We believe that this article will provide opportunities for future research on phishing in organizations.

Subjects Human-Computer Interaction, Computer Education, Security and Privacy
Keywords Phishing, Organization, Review, Social egineering

INTRODUCTION

Phishing is a devious and manipulative cybersecurity threat that targets organizations across all sectors worldwide (*APWG, 2023*), aiming at obtaining sensitive information, compromising systems, and securing financial gain. Organizations are faced with ongoing challenges in combating phishing because of the increase in the number of phishing attacks over the years along with continuous changes in attackers' strategies and tactics to get around security measures (*Cofense, 2023*). The implications of phishing attacks are damaging for organizations because they can lead to loss of revenue, reputations, and intellectual property with some of the attacks being used to initiate more complex cyber threats such as ransomware and data breach (*Verizon, 2022*). As a result, organizations have to defend against phishing attempts. They should adopt complete cybersecurity strategies, such as applying sophisticated technical defenses, educating staff members on security issues regularly, and creating guidelines and protocols for spotting and handling phishing attacks.

To enable organizations to fight against phishing, previous research studied phishing from several perspectives like developing interventions (*Franz et al., 2021*; *Goel & Jain, 2018*; *Singh & Meenu, 2020*), exploring human susceptibility to phishing (*Scott & Kyobe, 2021*), and analyzing phishing attacks (*T N, Bakari & Shukla, 2021*). Although these studies may provide a solid foundation on their own, combating phishing requires a multi-layer approach that focuses on applying several measures to make it harder for attackers to reach users and also implement all the reactive measures to reduce the damage and minimize its

Submitted 3 April 2024
Accepted 16 October 2024
Published 27 November 2024

Corresponding author
Kholoud Althobaiti,
kholod.k@tu.edu.sa

Academic editor
Yue Zhang

Additional Information and Declarations can be found on page 26

DOI **10.7717/peerj-cs.2487**

impact on organizations (*NSCS, 2018*). Therefore, exploring the diverse research landscape across various research disciplines can provide a holistic understanding of the fight against phishing in organizations. The rationale for this study arises from the increased number of such attacks. We believe that the systematization of existing literature would reveal the trend and gaps in the fight against phishing in organizations. Thus, our research aims to answer the following two questions:

RQ1: What are the current research directions targeting phishing in organizations?

RQ2: What are the open questions in the current literature for future research?

In this work, we provide a comprehensive systematization of organizational-oriented phishing research in terms of the process of handling phishing attacks in organizations from the first steps taken to protect organizations against phishing to the mitigation steps and learning from a successful attack (*SecAware, 2013*). We analyzed a total of 163 research papers published between 2012 and 2024 based on predetermined criteria, such as the use of organization-based keywords to ensure the study captures the spectrum of the organizational fight against phishing. The main contribution is the analyses of the existing literature which resulted in categorizing the studies based on the type of study and layer of protection. We found that the literature is heavily based on detecting phishing attacks and raising users' awareness with a limited number of studies on post-attack studies such as phishing incident response. This research is targeting cybersecurity professionals, researchers, and organizational decision-makers who are directly involved in the fight against phishing attacks.

The remainder of the article is organized as follows. First, we present the type of literature reviews done in the area along with a short background on the phishing life cycle. Second, we discuss the methodology adopted for this study followed by the results of the study. We then discuss the results and conclude the article.

BACKGROUND

To situate our research in the literature, this section discusses the previous review papers and taxonomies and explains a high-level description of the phishing life cycle that involves attack and defense in organizational settings.

Phishing taxonomies

Various taxonomies and classification schemes have been proposed to structure research on phishing attacks. One common phishing taxonomy considers the medium of the attack, target environment, and tactics by *AlEroud & Zhou (2017)* where *Goel & Jain (2018)* focused their review specifically on mobile phishing attacks as one common medium of phishing attacks. Social engineering attacks have been categorized based on their type: phishing, pharming, and spoofing (*Mathew, Al Hajj & Al Ruqeishi, 2010*). The mechanism-based review involves distinguishing between social engineering (*e.g.*, spam and phishing) and technical subterfuge (*e.g.*, impersonation) (*Gupta, Arachchilage & Psannis, 2018*), which is also can be categorized into conventional and automated techniques depending on the attacker's technicality (*Qabajeh, Thabtah & Chiclana, 2018*). *Gupta, Arachchilage & Psannis (2018)* proposed a taxonomy of various methods used to protect users from

technical and non-technical phishing attacks, which is categorized into user education, and automated detection of emails and websites. Automatic detection of phishing emails has been a popular area of study (*Muneer et al., 2021*), with some reviews specifically examining techniques such as machine learning-based detection (*Singh & Meenu, 2020*; *Gangavarapu, Jaidhar & Chanduka, 2020*), deep learning (*Dixit & Silakari, 2021*), and natural language processing (*Salloum et al., 2022*). Another study focuses on the countermeasures for a specific type of phishing, business email compromise (BEC), by categorizing its techniques and countermeasures (*T N, Bakari & Shukla, 2021*).

Additionally, user-centered phishing research has been approached from several perspectives. One study explored the literature to understand the characteristics and traits of phishing victims (*Darwish, Zarka & Aloul, 2012*), while another reviewed the human factors in phishing attacks (*Desolda et al., 2021*). User-centered interventions were examined by *Franz et al. (2021)*, analyzing existing approaches, attack vectors, and types of user interaction. Moreover, *Jampen et al. (2020)* and *Aldawood & Skinner (2018)* explored the effectiveness of security awareness programs in raising users' awareness.

The above reviews encompass general research on phishing that is targeted at both individuals and organizations. In our review, we focus on categorizing the literature on organizational-based research.

Phases of phishing attacks

A phishing attack is a social engineering attack that involves multiple phases of activities: the pre-attack phase, the attack phase, and the post-attack phase (*Alizadeh et al., 2023*). These phases may not occur only once but instead, they appear in a cyclical pattern.

The pre-attack phase involves activities aimed at exploring their goal, identifying a target, and learning more about them. Following the information gathering, the attacker can plan the strategy, technique, and the appropriate channel to achieve the goal (*Gupta et al., 2017*; *Thurman, 2020*; *Oest et al., 2018*; *AlEroud & Zhou, 2017*; *Alabdan, 2020*).

The attack phase includes the execution of the attack itself, which entails establishing communication and interaction with the target user and building a relationship. This process requires fabrication, such as impersonation and the use of false identifiers, to deceive the target (*Purkait, 2012*; *AlEroud & Zhou, 2017*) and persuade them to comply with the attacker to fall victim to the attack (*Parsons et al., 2015*; *Rader & Rahman, 2015*; *Benenson, Gassmann & Landwirth, 2017*).

The post-attack phase covers the exploitation of trust, the use of obtained information (*e.g.*, passwords or card details), or the exploitation of security vulnerabilities (*e.g.*, malware) at the appropriate time (*AlEroud & Zhou, 2017*; *Mouton et al., 2014*). This phase also includes covering tracks, which involves deleting event logs, fake accounts, or fake websites to remove evidence of the attack (*Shaikh, Shabut & Hossain, 2016*). It may also include blocking the user's access to their account by changing their passwords (*Qabajeh, Thabtah & Chiclana, 2018*; *Steer, 2017*; *Bursztein et al., 2014*; *Onaolapo, Mariconti & Stringhini, 2016*). The post-attack phase also involves ensuring the victim feels safe without noticing any suspicious activities and ensuring that the attackers achieved their goal (*Mouton, Leenen & Venter, 2016*).

Phases of phishing protection

Learning how attackers establish and execute phishing attacks helps organizations adopt and adapt frameworks and best practices (*Frauenstein & von Solms, 2009*; *Frauenstein & von Solms, 2013*; *Hammour et al., 2019*; *Moul, 2019*) to implement thorough countermeasures for protecting their assets and users. These measures encompass both proactive defenses, which are implemented before an attack, and reactive measures, which are taken during or after the attack.

Organizations primarily focus their proactive efforts on the early detection of phishing, often achieved through employee training and preventive technological measures (*Kokulu et al., 2019*). Some preventive technical measures include blocking emails before they reach the mail server (*Purkait, 2012*; *Park et al., 2014*) or blocking websites when a user's browser requests malicious content (*Frauenstein & von Solms, 2009*; *Tsalis et al., 2014*; *Jain & Gupta, 2016*). While these measures help detect phishing incidents, they cannot guarantee complete accuracy, necessitating concentrating efforts on training users to identify threats that may bypass these filters.

Cybercriminals continually seek new methods to evade proactive defenses, compelling organizations to establish reactive procedures for addressing new attacks. These reactive measures involve monitoring automated alarms, tracking user-reported phishing attempts, and scanning for suspicious activities (*Arachchilage & Cole, 2016*; *Abawajy, 2014*; *Arachchilage, Love & Maple, 2015*). Timely responses significantly aid organizations in responding to and minimizing the impact of attacks, thereby reducing the likelihood of potential victims engaging in phishing communications and mitigating harm to the organization.

While this provides an overview of the phishing life cycle, there is limited knowledge about the research conducted in the area including attacker strategies, users' awareness, interventions, challenges encountered during any of the phases, and incident handling within the organizational environment, specifically within information security centers.

METHODOLOGY

To understand the current landscape of phishing research focused on organizations, a systematic literature review was performed by following the guidelines of *Okoli (2015)*. Literature reviews are essential for advancing domain knowledge as they synthesize previous research and identify research gaps.

Selecting literature

Phishing is a highly prevalent topic that crosses multiple fields, resulting in papers published across various fields, including human–computer interaction (HCI), computer security, cryptography, and information systems. Consequently, three digital libraries were selected for the search: Association for Computing Machinery (ACM) Digital Library, Institute of Electrical and Electronics Engineers (IEEE) Xplore, and ScienceDirect.com, which cover the majority of relevant fields. The search keywords were consistent across databases and applied to titles, abstracts, or author-specified keywords (refer to Appendix for the queries used for each library).

In selecting keywords for the literature search, we focused on terms commonly found in recent studies on organizations. We initially experimented with a range of both broad and specific keywords to capture relevant research. This process was essential, given the extensive volume of phishing-related literature, which would otherwise result in an enormous number of articles to review. To be considered, articles had to include the term 'phish' or 'phishing' and one of the terms 'organisation', 'organization', 'institution', 'corporation', 'enterprise', 'workplace', or 'incident'.

Inclusion criteria

Using the search method outlined above, a total of 620 publications were initially identified, with some appearing in at least two libraries. The search was conducted on April 13, 2022. We then restricted the selection of articles from 2012 onwards to ensure the inclusion of recent research relevant to current challenges and advancements.

Extended abstracts, posters, and literature review papers were excluded to focus on peer-reviewed articles to focus on original research and empirical studies. We also limited the review to papers written in English.

After the initial exclusion and removal of duplication and unavailable 'pdf' files, 544 articles remained. The authors then commenced the full-text screening process by individually reading and analyzing the articles based on the following inclusion criteria: We included research specifically targeting or investigating organizational settings. More specifically, studies had to be tested in organizational environments or use data collected from specific organizations to ensure practical applicability. While many articles focused broadly on cybersecurity, we included only those that discussed phishing within the context of broader cybercrimes if they had dedicated sections addressing phishing specifically. Studies focusing on methods to prevent or remediate phishing, such as authentication mechanisms and anomaly detection systems, were also included to align with the study's objectives.

The full-text analysis further reduced the literature count by 105 articles.

The authors held several meetings during the screening process to ensure thoroughness and consistency in applying the inclusion criteria. These meetings helped to minimize biases and priming effects where discrepancies in article inclusion decisions were resolved through discussion and consensus to ensure reliability and validity in the selection process.

After writing the article, we researched the literature on June 10, 2024, to include any missing papers. The same screening process was applied to the new literature, resulting in 58 additional studies, increasing the total number of studies reviewed to 163 studies. Figure 1 summarizes the entire process of selection of publications.

A TAXONOMY OF ORGANIZATION-BASED PHISHING RESEARCH

While reviewing the literature, we observed a variation in themes concerning the underlying stage of the attack and defense life cycle. After several discussions among the researchers, we chronologically categorized the literature starting with the proposal of policies and frameworks and then the factors that affect the susceptibility to phishing, testing of user

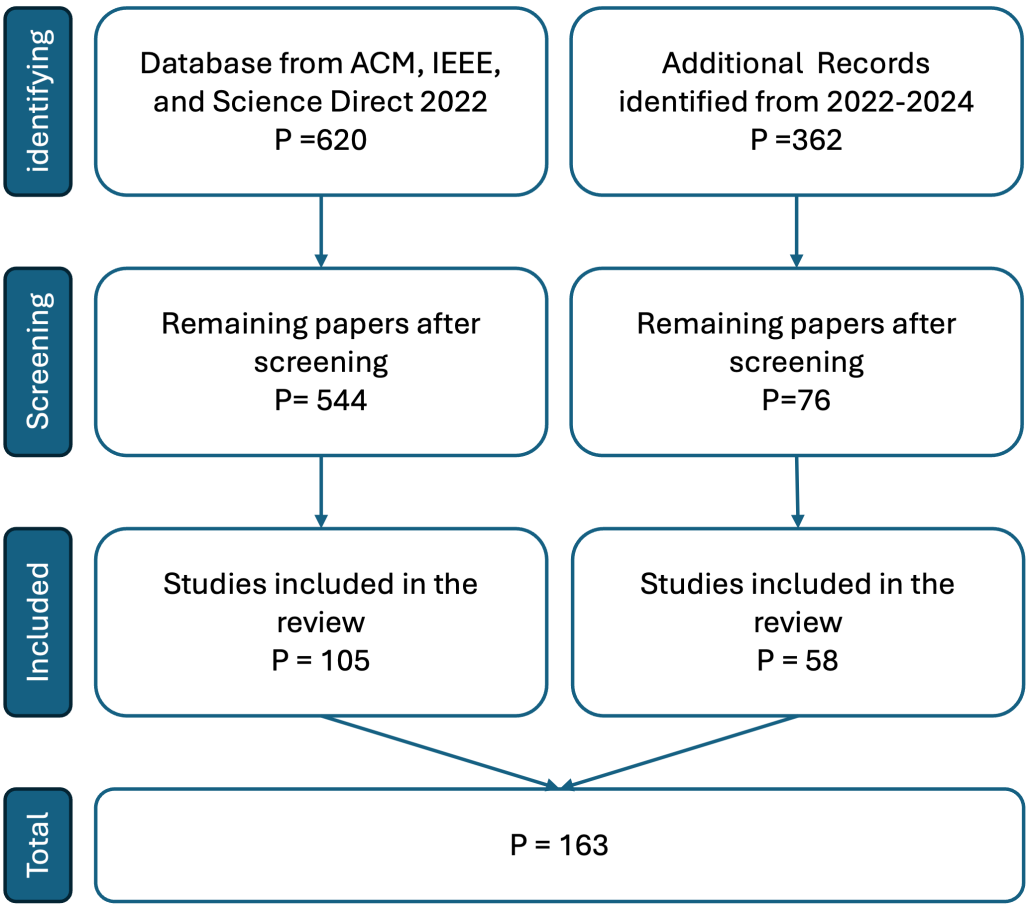

Figure 1 **The literature screening process.**

Full-size DOI: 10.7717/peerjcs.2487/fig-1

awareness, and interventions used to raise their awareness, the detection of phishing communications, and research on incident response to phishing attacks, find the list of categories in Fig. 2 and a summary of the findings in Table 1.

Policies and frameworks

Organizations are required by law to comply with the government-imposed cybersecurity regulations, which are found to raise organizations' awareness of threats and positively affect companies' decisions to invest in IT and security, as seen in Michigan and Oregon organizations (*Wang et al., 2024*). Therefore, well-established cyber security frameworks such as COBIT, NIST, and ISO27001 complement the regulations by offering a comprehensive approach.

Prior research also proposed policies and frameworks to defend the organization's ecosystem specifically from phishing attacks. As an example suggesting organizational compliance with training employees, educating them, and banning the sharing of passwords and sensitive information (*Itani et al., 2024*). One of the studies focuses its framework on the relation between key elements attackers aim to exploit: human factors, organizational

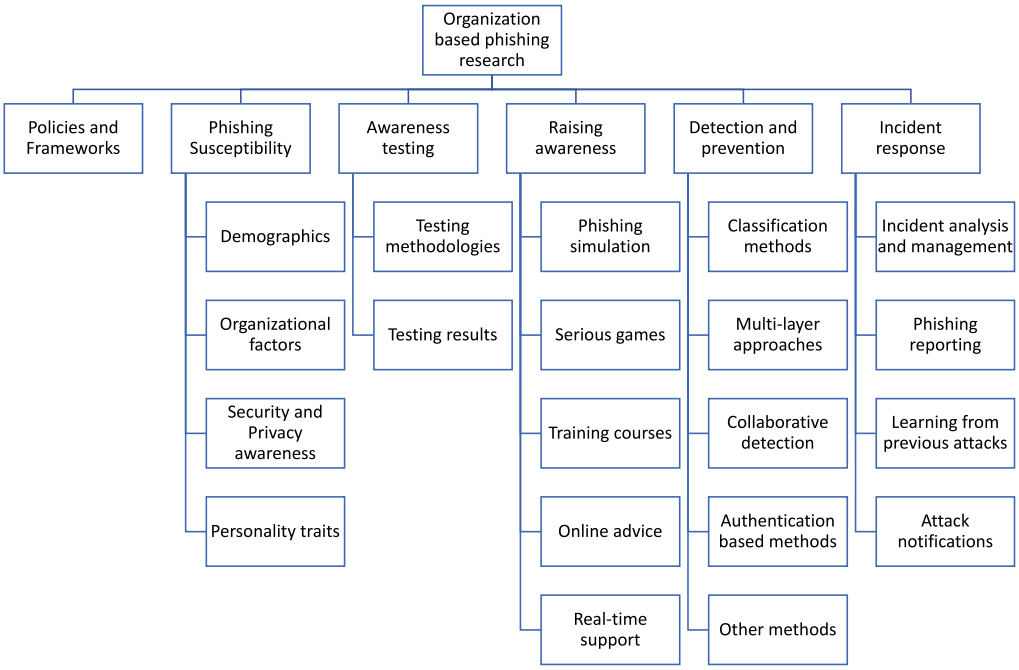

Figure 2 **The resulted taxonomy of organization-based research.**
Full-size DOI: 10.7717/peerjcs.2487/fig-2

aspects, and technological controls (*Frauenstein & von Solms, 2014*). This relationship involves the use of best practices such as COBIT to identify suitable technological techniques, the assurance of adequate policies and procedures to dictate the employees' behavior, and teaching employees how to use the organizations' technological controls. Whereas another study focused only on the human factor element by proposing an AI-based user and entity behavior analytics framework that helps analysts assess each user's exposure to threats based on real-world data (*Calvo et al., 2023*). This approach identifies potential vulnerabilities before attacks happen and allows organizations to prioritize their security efforts and implement preventive measures.

The size of the organization plays an important role in the framework used because small and mid-sized organizations, although targeted by phishing attacks, they have limited budgets with restricted resources, requiring them to size up their budget to the needed security investment. *Rodríguez-Corzo, Rojas & Mejía-Moncayo (2018)* proposed a phishing model that focuses on three actors: business, technology, and people. For the business factor, the business characteristics, threats, and the attacker purpose should be identified because they will be utilized in the technology factor by identifying its current status and resources needed to implement the model. The third actor is people who are the training staff and their exposure to risk based on their position.

Other studies focus their framework or policy on specific types of phishing attacks or vulnerabilities. *Shakela & Jazri (2019)* proposed a Spear Phishing Exposure Level (SPEL) framework to assess and reduce spear phishing-related threats, which is designed from two perspectives: the threat source and vulnerability to threats. This approach allows

Table 1 Summary of organization-based phishing research.

Category	Subcategory	Findings
Policies and frameworks		- Cybersecurity law & frameworks influence organizational awareness of security. - Policies focus on training, data protection, and vulnerability checks. - Organization size plays a role in cybersecurity decisions.
Phishing susceptibility	Demographics	- While age and major is a susceptibility factor, gender has no impact.
	Organizational factors	- Overconfidence in security and distractions increase risk. - Tenured employees, managers, and tech staff have higher awareness. - Level of awareness differs between sectors
	Awareness	- Security awareness and knowledge reduce risk.
	Personality traits	- High conscientiousness and low agreeableness and trust reduce vulnerability. - High Influence decreases risk compared to high Dominance.
Awareness testing	Methodology	- Phishing simulation is most common compared to surveys. - Choice of the methodology is cultural-dependent.
	Results	- High success rates of phishing attacks requiring better training.
Raising awareness	Phishing simulation	- Targeted simulations reduce susceptibility and increase reporting. - Limited effectiveness for users already vulnerable. - Challenges include data privacy and management in large organizations.
	Serious games	- Employ personality traits, role-playing scenarios, and quizzes. - Awards and sanctions increase engagement.
	Training courses	- Commonly integrated into curricula and IT programs. - Combining theoretical training with other methods increases effectiveness.
	Online advice	- Social networks can be used as source for online advice. - Public anti-phishing web pages lack clear, concrete advice.
	Real time support	- Security nudges and extensions improve phishing detection. - user-centric tools are needed for real-time support.
Detection and prevention	Classification methods	- Common methods are machine learning, deep learning, clustering, and NLP.
	Multi-layer methods	- Multi-layer integration increases the classification accuracy. - Additional layers include IP mapping, logo recognition, and dynamic firewall rules
	Collaborative detection	- Information sharing between organizations can improve defense measures. - Privacy-preserving protocols for secure data queries.
	Authentication	- Email authentication protocols help but have a low adoption rate - Dynamic passwords, brand indicator authentication, and nonce message protocols enhance phishing prevention.
	Other methods	- Various methods such as detecting bogus invoices, QR code manipulation, malicious executable files, ransomware, and lateral phishing. - Virtual honeypots to block access to phishing sites. - Detection of encrypted phishing sites, domain-based brand protection, and multi-stage site takedown enhance security.

(*continued on next page*)

Table 1 (*continued*)

Category	Subcategory	Findings
Incident response	Attack insights	-Frequent analysis of attacks enhances protection against increasingly sophisticated attacks.
	Notifications	- Notification about ongoing attacks has limited effect.
	Incident management	- Incidents analysis tools increase situational awareness. -Attack modeling techniques enhance risk assessment and response strategies.
	Reporting attack	Phishing reporting enhances response time and resilience while reducing security costs.

organizations to determine the possibilities of attack in the absence of security mechanisms. *Ismail et al. (2017)* proposed a policy to mitigate the impact of watering attacks and spear phishing; both allow the attacker to take control of an insider account. After surveying business stakeholders, the authors found that role-based access control is not enough if the attack originates from a compromised insider. Therefore, they first proposed adding another access control layer, such as Bell La-Padula, which uses access labels on objects and clearances for subjects to reduce the impact of unauthorized access. Then they proposed policies include setting complex passwords, reporting lost devices, disabling the ability to install apps from a third party, enforcing the installation of anti-viruses and firewalls on personal devices, disallowing the use of jailbroken or rooted personal devices to connect to organization facilities and only allowing activated accounts to be connected *via* wireless. To evade phishing attacks in traditional tender allocation systems, *Dubey et al. (2023)* proposed using blockchain along with common security practices through smart contracts and immutable records, which contribute to ensuring fair competition by automating the tender process from creation to winner selection. For bring-your-own-device environments, *Bann, Singh & Samsudin (2015)* propose a multi-level security and access control policy based on the analysis of four well-established security policies namely, mandatory access control (MAC), Clark Wilson, Low Water Mark access mandatory control (LOMAC), and attribute-based access control (ABAC) based on various quality metrics, such as the size of the organization, the cost of administration, and complexity. To evaluate the applied cyber security frameworks in defending against phishing, *Kulkarni et al. (2024)* suggested the use of tools such as *HiddenEye* and *sendemail* in a simulated environment can asses with phishing countermeasures.

Phishing susceptibility

Crafting phishing attacks often relies on a common method that is referred to as social engineering, which uses psychology and behavior to make emails seem more trustworthy and discourages people from carefully checking the information they receive. This approach increases the probability of successful attacks. While the previous theme examined attacker strategies used in real attacks, in this theme, we discuss the research that addresses the technical and human factors related to phishing susceptibility.

Demographics. Studies show that demographics are a significant factor in determining individuals' susceptibility to phishing attacks. A study of university students in Emirates showed that junior students are less likely to fall victim to phishing than senior

students (*Mohebzada et al., 2012*). Likewise, an investigation of multi-national financial organizations revealed that older participants are more vulnerable to phishing than younger participants (*Taib et al., 2019*). This observation was ascertained in several companies from various sectors (*Lain, Kostiainen & Čapkun, 2022*); however, this correlation was not observed with users of privacy-preserving technology companies (*Clark, 2012*). Younger users are more susceptible at the early stages (receiving and opening emails), whereas older users are more likely to fall victim at advanced stages (*e.g.*, visiting phishing sites) (*Zhou, Zhang & Liu, 2023*). Considering the variation in studies' results, we can attribute this to differences in participants' age ranges, with some studies focusing on ages 18 to 25, while others include participants up to 40.

On the other hand, empirical studies have found that gender does not have a statistically significant impact on one's likelihood of falling victim to an attack (*Mohebzada et al., 2012*; *Taib et al., 2019*; *Flores, Farid & Samara, 2019*; *Clark, 2012*; *Zhou, Zhang & Liu, 2023*; *Lain, Kostiainen & Čapkun, 2022*; *Ribeiro, Guedes & Cardoso, 2024*) except for a study in a Philippine university showing higher awareness of spam (*Hermogenes & Capariño, 2019*). Thus, while age remains a crucial factor in identifying those at greater risk, gender does not appear to influence susceptibility to phishing.

Regarding the university major, studies showed that IT students have a higher awareness of phishing emails and cybercrimes compared to their peers in education and science fields (*Manasrah, Akour & Alsukhni, 2015*); likewise, they have the best resistance against phishing attacks (*Andrić, Oreški & Kišasondi, 2016*). Similarly, 54.32% of IT students were aware of spam and phishing compared with students from teaching education programs (*Hermogenes & Capariño, 2019*), signifying the importance of technology competencies in phishing susceptibility (*Ribeiro, Guedes & Cardoso, 2024*). This finding is contrasted by *Clark (2012)*, who reported an absence of correlation between an employee's field of study in the US, whether computer-related or not, and their susceptibility to phishing attacks in experimental settings. These contrasting results highlight a complex landscape of cyber literacy and vulnerability among university students, suggesting that awareness does not necessarily equate to immunity from cyber threats.

Organizational-based factors. Several key elements are found in the analyzed literature. The strong belief in organizations' security measures may lead to a lower sense of risk (*Kearney & Kruger, 2014*) as observed in interviews with banking IT staff who assumed that their security protocols would prevent attacks or quickly rectify its implications (*Conway et al., 2017*).

Additionally, the length of time employees had worked at the company played a role. Newer employees, especially those in their first year, were found to be more vulnerable to phishing attempts than their more tenured colleagues (*Kearney & Kruger, 2014*). This finding was supported by a large-scale simulation in financial organizations (*Taib et al., 2019*) and a field experiment at a university and a large international consultancy company (*Burda et al., 2020*).

Furthermore, job responsibilities influenced vulnerability to phishing; thus, employees with managerial duties tended to be more cautious, potentially due to their investment in

the company's image or the consequences of non-compliance (*Taib et al., 2019*; *Eftimie et al., 2021*). Additionally, employees with higher effective organizational commitment show higher awareness in various Australian organizations (*Reeves, Parsons & Calic, 2020*). For example, employees from technology-based departments have a higher level of awareness than those from social-based departments in a Thai organization (*Daengsi et al., 2021*). Also, job roles that utilize a centralized inbox lead to increased exposure to potential phishing emails due to the nature of such inboxes (*Williams, Hinds & Joinson, 2018*). Apart from the job roles, generally, the frequent use of general computers and usual internet routine reduce employees' susceptibility to phishing (*Ribeiro, Guedes & Cardoso, 2024*; *Lain, Kostiainen & Čapkun, 2022*).

The susceptibility to phishing was also examined between sectors. Government employees have more knowledge of phishing protection than employees from private sectors in Saudi Arabia (*Innab et al., 2018*). Adding to that, employees associated with privacy-preserving technology companies in the US are still likely to disclose personal information in phishing scenarios (*Clark, 2012*).

Interruptions during tasks increase the likelihood of employees falling for phishing scams, as they may be less focused and thus more susceptible to fraudulent communications (*Williams, Morgan & Joinson, 2017*).

The importance of organizational norms in influencing employees' compliance with information security policies (ISPs) has been highlighted by *Petrič & Roer (2022)* and *Williams, Hinds & Joinson (2018)*. The study provides comprehensive knowledge of how many normative variables, in particular phishing vulnerability, affect employees' conduct. Notably, the investigation shows that the effect of descriptive norms on the tendency of staff members to click on questionable links differs from the effect of personal norms in the same tendency. It has been shown that workers who adopt security-promoting norms are less likely to interact with phishing emails and to exercise caution when clicking on embedded links. The research suggests that a moral commitment to organizational security norms triggers more analytical processing of emails. However, this commitment may not always safeguard against sophisticated phishing tactics post-click.

These results imply that evaluating and mitigating phishing susceptibility in an organizational setting requires a comprehensive approach that takes into account variables including job role, tenure, perceived security strength, and organizational norms.

Security and privacy perception and knowledge. The perception and knowledge of security and privacy can play a crucial role in an individual's susceptibility to cyber threats. A study of Middle Eastern countries revealed that the perceived high-security risk does not always translate to protective actions as the participants may fall prey to phishing (*Aleroud et al., 2020*). Similarly, in Australia, individuals with a lower fear of cyber threats exhibited better information security awareness (*Reeves, Parsons & Calic, 2020*; *Ribeiro, Guedes & Cardoso, 2024*).

Furthermore, a lack of security knowledge, such as misunderstanding security indicators on websites, leaves users more open to deception by phishers who often exploit such gaps in knowledge (*Aleroud et al., 2020*; *Williams, Hinds & Joinson, 2018*). Knowledge of the

difference between HTTP and HTTPS and URL syntax and shorteners can help university students avoid suspicious emails (*Andrić, Oreški & Kišasondi, 2016*). A lack of technical understanding about what spear phishing entails, how personal information is used in attacks, and the consequences of engaging with phishing emails can lead to increased susceptibility (*Williams, Hinds & Joinson, 2018*), especially for financial consequences (*Aleroud et al., 2020*). Knowledge of red flags in phishing emails, such as spelling errors and sender address is critical (*Williams, Hinds & Joinson, 2018*; *De Bona & Paci, 2020*; *Buckley et al., 2023*). While this knowledge can be effective and used by several users, they might be misleading in the occurrence of lateral phishing, requiring knowledge of the sender's writing style and the expectation of communication topic (*Chitare, Coventry & Nicholson, 2023*).

Higher privacy behavior reduces individuals' susceptibility to phishing (*Zhou, Zhang & Liu, 2023*), particularly among women in the Middle East, influencing their willingness to share personal details; however, this caution does not necessarily extend to protecting them from phishing (*Mohebzada et al., 2012*; *Aleroud et al., 2020*).

Although raising knowledge of security and privacy is critical, it does not always protect against phishing, signifying the need for improving security procedures and education.

Personality traits. The Big Five personality traits have been linked to various behaviors concerning vulnerability to phishing. Highly conscientious individuals typically engage in responsible security practices, whereas those with lower levels of conscientiousness are prone to riskier behaviors (*Eftimie et al., 2021*). Similar to the findings above, those in leadership positions, often characterized by low levels of agreeableness and high levels of conscientiousness, are less likely to fall for phishing attacks (*Eftimie et al., 2021*; *Yaser Al-Bustani et al., 2023*). Regarding trust, it significantly affects vulnerability to spear phishing; especially in Middle Eastern countries. Phishers usually exploit trust, particularly through credible-looking and contextually convincing materials, which underline the intricate link among personality, trust, and susceptibility to phishing (*Aleroud et al., 2020*). Experimenting with financial organizations shows that employees with higher trust in their intuition are less likely to engage with phishing emails (*Buckley et al., 2023*). In addition, individuals' self-efficacy in detecting phishing attempts demonstrated a significant influence on their susceptibility to phishing attacks (*Ribeiro, Guedes & Cardoso, 2024*). People with high Influence are less susceptible to phishing due to their social awareness and caution, those with high Stability are moderately resistant but still have some vulnerabilities, while individuals with high Dominance are more susceptible because they prioritize results over careful scrutiny (*Yaser Al-Bustani et al., 2023*).

Phishing awareness testing

Awareness testing in organizations is a critical component of cybersecurity strategy, particularly in addressing the susceptibility of individuals to phishing attacks. This testing is conducted using a variety of methodologies, each revealing distinct aspects of human vulnerability and behavioral tendencies in the context of cyber threats.

Testing methodology. To assess and enhance awareness, previous research employed various methodologies. The most common methodology is the *phishing simulation experiments* (*Bakhshi, 2017*; *Blancaflor et al., 2021*; *Bakar, Mohd & Sulaiman, 2017*). An example is sending an email asking the employees to click on a link to a survey (*Bakhshi, 2017*; *Blancaflor et al., 2021*). The success of these simulated attacks can reveal the extent of vulnerability among the participants. To boast the benefits of such methodology, *Rutherford, Lin & Blaine (2022)* utilized the machine learning algorithms to understand the simulation results based on the potential victim's demographics and administrative data.However, setting up simulated phishing experiments to measure actual behaviors is not only expensive but also raises ethical concerns, such as user consent.

Surveys developed to gather information can precede simulated phishing attacks. For example, researchers in Manila collected personal details through a survey and then used this information to launch targeted phishing attacks (*Blancaflor et al., 2021*). In some cases, surveys can effectively replace simulation methodologies. The results of an experiment in an Indonesian government sector revealed a significant relationship between the simulation results and the questionnaire results (*Ikhsan & Ramli, 2019*). However, *Flores et al. (2015)* suggested that the methodology used is dependent on the culture as surveys can be used as a proxy to measure employees' intention to avoid social engineering in Sweden while scenarios are the best proxy in American culture, indicating that the use of assessment methods can differ between national cultures. Another method to test users' awareness is the use and development of standard scales. A phishing experiment with Australian students revealed that students who achieved high scores in the experiment also achieved a high score on the Human Aspects of Information Security Questionnaire (*Parsons et al., 2017*).

Testing results. Several studies have highlighted how surprisingly easy it can be to execute successful phishing attacks within organizations. For instance, in a branch office of a cooperative organization, a significant number of employees were comfortable sharing sensitive information, such as details about office supplies and equipment (*Bakhshi, 2017*). This finding underscores a lack of awareness regarding the sharing of potentially sensitive information. In a mid-sized university, 44.3% of users clicked on at least one phishing email, with 18.6% entering valid credentials (*Cuchta et al., 2019*); similarly, 42% of students in another experiment visited and completed forms and downloaded the email attached image (*Rastenis et al., 2019*). In total, 38% in a Malaysian university also entered their work ID and password, and 95% agreed to receive the financial aid (bait) (*Bakar, Mohd & Sulaiman, 2017*). This pattern of failure is not that different in surveys where 25% of students failed to correctly identify phishing emails in the survey (*Andrić, Oreški & Kišasondi, 2016*). A long-term study in various sectors revealed that about 32% will fall for phishing at least once if exposed to phishing emails (*Lain, Kostiainen & Čapkun, 2022*). These high engagement rates with phishing attempts indicate a substantial gap in awareness and the ease with which attackers can exploit this vulnerability. Studies in higher education institutions have shown that a large portion of students and employees are influenced by

phishing emails, with a notable percentage of them providing personal data. This finding suggests a need for enhanced security education and training.

Raising users awareness

The field of raising phishing awareness in organizations has seen extensive research, addressing various methodologies and their effectiveness such as instructor-led, video-based, text-based, and game-based training along with real-time support. Although the delivery approach is important, *Alkhazi et al. (2022)* observed that the enjoyable training sessions encourage Kuwaiti government employees to engage in self-learning and future training. To design the awareness materials, most of organizations rely on experts to tailor the content but some use non-expert crowd-sourcing participants to identify the common phishing cues that can be used in training based on the recent phishing attacks. This method helps provide training from the perspective of the system end-users capable of providing fresh, diverse, and comprehensive phishing cues over time (*Rosser et al., 2022*).

Phishing simulation for training. Simulated phishing exercises are also used to train employees to recognize and respond to phishing attempts. This method involves creating and sending simulated phishing emails to employees, which mimic the tactics and appearance of real phishing emails, but without the malicious intent. The goal is to expose employees to the types of phishing that they might encounter in a safe and controlled environment. Such studies were explored in several sectors and countries such as transportation in Bangkok (*Sirawongphatsara et al., 2023*), various small Japanese organizations (*Higashino et al., (2019)*, healthcare sector (*Williams, Zafar & Gupta, 2024*), and Israeli financial institution (*Hillman, Harel & Toch, 2023*). A notable finding across several studies, including research in Italy (*De Bona & Paci, 2020*) and the USA (*Pirocca, Allodi & Zannone, 2020*), shows that targeted simulated phishing training reduces susceptibility compared with generic phishing training (*McElwee, Murphy & Shelton, 2018*) with a noticeable increase in phishing reporting rate (*Hillman, Harel & Toch, 2023*). However, analysis of mid-sized and large companies demonstrates this method's limited effectiveness for those already susceptible to phishing (*Siadati et al., 2017*; *Lain, Kostiainen & Čapkun, 2022*). Other research explored combining the phishing simulation with rewards and sanctions in organizations to mitigate risky behavior (*Blythe, Gray & Collins, 2020*; *McElwee, Murphy & Shelton, 2018*).

Although this type of training is effective in raising awareness, it is challenging to run; for example, using the open-source framework raises concerns about exposing staff information suggesting storing users' data locally rather than using public servers (*Higashino et al., 2019*). If run locally without tools, it is overwhelming to manage in large organizations (*Althobaiti, Jenkins & Vaniea, 2021*).

Serious games. Serious games are typically employed in various fields. Serious games include interactive games for education and training. *Pantic & Husain (2018)* applied the Five-Factor Model of personality traits to correlate types of phishing emails with individual vulnerabilities, suggesting a more personalized approach for training. *Underhay, Pretorius & Ojo (2016)* proposed a game-based e-learning model for university technology students

in South Africa. The game involves role-playing as a system administrator, requiring players to secure networks and systems. *Gupta et al. (2020)* developed a serious game for cybersecurity professionals to identify sophisticated phishing emails using a mix of quizzes and feedback mechanisms. Similarly, *Birajdar & T N (2022)* developed a serious game for IT professionals that concentrates on aspects such as interactivity, depth of knowledge, awards, and sanctions.

Phishing training courses. Phishing training is used for various purposes, such as educational curricula and IT training programs. *Turner & Turner (2019)* integrated phishing awareness modules into social studies classes, demonstrating positive outcomes in understanding and preventing phishing attacks. Interactive tools and apps are used to provide training in order to increase awareness among students and professionals in American high schools (*Podila et al., 2020*) and various sectors in Qatar (*Al-hamar & Kolivand, 2020*). This type of training is also used for helping cybersecurity students efficiently create spear phishing attacks, such as developing the Social Engineering Vulnerability Evaluation (SiEVE) process, a method for identifying targets, profiling them, and crafting highly personalized social engineering attacks (*Meyers et al., 2018*).

Combining theoretical training with practical training in a medical organization in the Slovak Republic improved phishing awareness to 13% (*Madleňák & Kampová, 2022*). Additionally, combining two or more training methods can effectively enhance security awareness, such as providing text-based training along with gamification (*Alkhazi et al., 2022*). For example, due to the limited resources in small-sized universities, *Matovu et al. (2022)* incorporated the in-class lectures for training combined with after-training Kahoot!-based games.

However, even after employing security training, a significant proportion of employees are still vulnerable to phishing (*Kearney & Kruger, 2014*; *Madleňák & Kampová, 2022*), indicating the need for long term awareness plan.

Online phishing advice. The use of Twitter-based awareness strategies for bank customers in the Emirates revealed that while there is increased use of social media for fraud awareness, the impact and clarity of the advice vary (*Skula, Bohacik & Zabovsky, 2020*). *Mossano et al. (2020)* analyzed the publicly available anti-phishing web pages and found a lack of inconsistencies and concrete advice (*Mossano et al., 2020*).

Real time support. Previous research examined the impact of providing support to users when they encounter potential phishing attempts. The use of security nudges (*e.g.*, highlighting the sender) improves individuals' detection of phishing emails (*Nicholson, Coventry & Briggs, 2017*). Similarly, using the EyeBit extension that deactivate all the forms inputs if the user did not look at the address bar underscores the importance of real-time, user-centric tools in combating phishing (*Miyamoto et al., 2014*).

The real-time support that is coming from peers and family was studied by *Coronges et al. (2012)*. They studied the impact of social networks on mitigating the spread of phishing attacks, investigating whether warnings from friends or superiors are more effective in preventing successful phishing incidents. However, highly central individuals did not warn

others about phishing attacks, meaning these networks are ineffective. Adding a warning on the top of a suspicious email as real-time support intervention significantly reduces phishing clicks and dangerous actions, though the length of the warning has no significant difference in the click rate (*Lain, Kostiainen & Čapkun, 2022*).

Phishing detection and prevention

Previous research has explored a diverse range of approaches and technologies to combat phishing attacks using various attack vectors and methods, aiming at improving the organizations from phishing attacks across different vectors including websites (*Oest et al., 2019*; *Cuzzocrea, Martinelli & Mercaldo, 2018*; *Chen et al., 2021*; *Aslam & Nassif, 2023*), emails (*Stembert et al., 2015*; *Sanchez & Duan, 2012*; *Vos, Erkin & Doerr, 2021*; *Lam & Kettani, 2019*; *Lee et al., 2021b*; *Zeng, 2017*), voice phishing (*Yu et al., 2024*), and job advertisements posted on a popular Australian platform (*Mahbub, Pardede & Kayes, 2022*), with some of these studies focus on accuracy against specific characteristics such as languages (*Dunder, Seljan & Odak, 2023*; *Yu et al., 2024*). Notably, the approaches discussed concentrate on protecting organizations, utilizing organizational data, and improving the usability of phishing detection systems, such as using an interactive website to ease scanning and enhance the classifier accuracy (*Shombot et al., 2024*).

Classification based measures. Classification-based methods are widely employed for detecting phishing attacks. These methods leverage various classification techniques such as machine learning (*Mahbub, Pardede & Kayes, 2022*), deep learning (*He et al., 2024*; *Devalla et al., 2022*), natural language processing (*Dunder, Seljan & Odak, 2023*; *Tudosi et al., 2023*), computer vision (*Pires & Borges, 2023*). These classification methods utilize a wide range of features such as URL-based features (*Swarnalatha et al., 2021*; *Devalla et al., 2022*; *Bouijij, Berqia & Saliah-Hassan, 2022*; *Aslam & Nassif, 2023*), image-based features extracted from websites screenshots (*Tanimu & Shiaeles, 2022*), websites cost features (*Ito, Takata & Kamizono, 2022*), and social features extracted from LinkedIn profiles (*Dewan, Kashyap & Kumaraguru, 2014*). For detecting voice phishing calls, *Yu et al. (2024)* explored several classifiers such as XGBoost, SVM, and Random Forest and found that combining Named Entity Recognition (NER) with sentence-level N-gram techniques improves the classification performance, particularly in reducing false negatives. In addition, some papers utilized feature detection algorithms such as Oriented FAST and Rotated BRIEF (ORB) algorithms for logo detection and localization (*Bhurtel, Siwakoti & Rawat, 2022*). Studies have focused on balancing data to enhance model accuracy using techniques like SMOTE (*Alsubaei, Almazroi & Ayub, 2024*; *Tamanna et al., 2024*).

Random forest and XGBoost have been used effectively on datasets such as URLs, websites, and job ads, achieving accuracies as high as 98.37% in certain cases (*Devalla et al., 2022*; *Aslam & Nassif, 2023*; *Tamanna et al., 2024*; *Dewan, Kashyap & Kumaraguru, 2014*). Support vector machines (SVM), KNN, and decision trees are also popular classifiers for phishing detection, with varying levels of success, reaching up to 94.87% accuracy (*Shombot et al., 2024*; *Mahbub, Pardede & Kayes, 2022*). Neural networks, particularly BiLSTM and ANN, show significant potential in URL and email phishing detection,

Table 2 Summary of studies on phishing classification.

Method	Data type	Classifier	Accuracy	Citation
Deep learning	URL or website	ANN	90.82%	*Devalla et al. (2022)*
		BiLSTM	94.41%	*Devalla et al. (2022)*
		DNN	99.27%	*Bouijij, Berqia & Saliah-Hassan (2022)*
		ResNeXt-embedded GRU	98.00%	*Alsubaei, Almazroi & Ayub (2024)*
		CNN	95.76%	*Pires & Borges (2023)*
	Emails	LSTM & XGBoost	98.59%	*He et al. (2024)*
Machine learning	URL or websites	Random forest	95.04%	*Devalla et al. (2022)*
			98.37%	*Aslam & Nassif (2023)*
			95.00%	*Ito, Takata & Kamizono (2022)*
		XBoost	94.20%	*Devalla et al. (2022)*
		AdaBoost	82.36%	*Devalla et al. (2022)*
		KNN	90.47%	*Devalla et al. (2022)*
			94.87%	*Aslam & Nassif (2023)*
		SVM	84.50%	*Shombot et al. (2024)*
			91.49%	*Aslam & Nassif (2023)*
		Random tree	95.98%	*Aslam & Nassif (2023)*
		Extra-Tree	98.77%	*Bouijij, Berqia & Saliah-Hassan (2022)*
		Multi-layer perceptron	96.71%	*Aslam & Nassif (2023)*
	Email	Local outlier factor	–	*Wu & Guo (2022)*
		SVM	98.70%	*Sanchez & Duan (2012)*
		Random forest	98.28%	*Dewan, Kashyap & Kumaraguru (2014)*
		Decision Tree	97.32%	*Dewan, Kashyap & Kumaraguru (2014)*
		Naive Bayesian	69.35%	*Dewan, Kashyap & Kumaraguru (2014)*
		Decision table	95.05%	*Dewan, Kashyap & Kumaraguru (2014)*
	Financial transactions	XBoost & Random Forest	94.00%	*Tamanna et al. (2024)*
	Job ads	Random forest	91.80%	*Mahbub, Pardede & Kayes (2022)*
		J48 Decision tree	91.64%	*Mahbub, Pardede & Kayes (2022)*
	Financial website	Logistic regression	97.30%	*Yu et al. (2024)*
		SVM	97.00%	*Yu et al. (2024)*
NLP	Email& Domains	Statistical classifier& NLPRank	–	*Thejaswini & Indupriya (2019)*
Clustering	URL or websites	Agglomeration clustering & K-medoids	–	*Zhuang et al. (2012)*

with accuracies reaching up to 99.27% (*Bouijij, Berqia & Saliah-Hassan, 2022*; *Alsubaei, Almazroi & Ayub, 2024*; *Pires & Borges, 2023*). Heuristic approaches complement these methods by identifying phishing through analyzing sender information (*Sanchez & Duan, 2012*) and applying the local outlier factor on email headers from mirrored SMTP network traffic (*Wu & Guo, 2022*). NLP is explored for detecting various attacks, including phishing emails, through email content and source URL analysis (*Thejaswini & Indupriya, 2019*). Hierarchical clustering and K-medoids have been used to develop automatic categorization systems for grouping phishing websites or malware based on shared characteristics (*Zhuang et al., 2012*). The list of studies with their results are summarized in Table 2.

Multi-layer classification methods. Some studies integrate multiple approaches, such as using K-nearest neighbors, and IP-based mechanisms, focusing on IP mapping and logo recognition (*Bhurtel, Siwakoti & Rawat, 2022*), or machine learning algorithms with dynamic firewall rule generation (*Tudosi et al., 2023*). Similarly, the use of the naive Bayesian classifier, fuzzy string comparison, and image hashing results in 95% detection of fake educational domains (*Privalov & Smirnov, 2023*; *Privalov & Smirnov, 2022*). Classifying phishing websites using blacklists alone is not effective as they are not effective against zero-day attacks and cloaked phishing sites (*Oest et al., 2019*; *Chen et al., 2021*). Though, phish Mail Guard integrates blacklist, white list, heuristic techniques, DNS, and textual content analysis for comprehensive phishing email identification (*Hajgude & Ragha, 2012*). *Varshney et al. (2021)* proposed a novel method to uncover DNS over HTTPS traffic for phishing detection. Another study is NoFish, where (*Niroshan Atimorathanna et al., 2020*) combined various mechanisms like URL analysis, visual similarity detection, DNS phishing detection, and an email client plugin. It utilizes machine learning, natural language processing (NLP), and computer vision techniques to detect phishing attacks, achieving an accuracy of 94% for URL detection and 91.67% for email detection. Using information from software-defined networking through deep packet inspection with the help of NNA resulted in an average accuracy of 98.1% (*Chin, Xiong & Hu, 2018*). Heuristics also was used by *Liu & Zhang (2012)*. They proposed two layers of detection where they first compute the weight for the URL features. If the weight does not exceed a threshold, they check the webpage features, providing specialized detection mechanisms for financial phishing.

Collaborative phishing detection. Collaboration between organizations can effectively defend against phishing. *Higashino (2019)* designed a system for sharing information about phishing attacks across financial organizations. *Vos, Erkin & Doerr (2021)* presented a privacy-preserving protocol for querying multiple data providers without revealing stored data. Similarly, *Deval et al. (2021)* employed machine learning methods for collaborative phishing detection, allowing for the inclusion of new features in the models while *Salau, Dantu & Upadhyay (2021)* utilized blockchain technology to share data about phishing between organizations. Interestingly, *Stembert et al. (2015)* proposed a method that combines interaction methods to detect email phishing attacks, leveraging the intelligence of both expert users and novice users.

Authentication based prevention. Email spoofing techniques such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) help IT staff in organizations to verify the authenticity of the sender's domain to prevent malicious actors and countermeasures phishing emails (*Kulkarni et al., 2024*). However, these protocols have a low adoption rate because of the deployment technical issues, weak incentives, and concerns about blocking legitimate emails (*Hu, Peng & Wang, 2018*), requiring applying other methods to complement them. Similarly, the security multi-factor authentication method–Fast Identity Online 2 protocol was found to be challenging to deploy with concerns of security,

usability, and adaptability in real-world enterprise use cases (*Kepkowski et al., 2023*). Recent studies proposed several authentication solutions, such as the use of dynamic password technology as an alternative to OTP, offer new avenues for preventing phishing attacks (*Xu, Qi & Xi, 2016*) and the brand indicator for message identification to complement the sender's email domain with their organization authenticated logo (*Dolnák & Kampová, 2022*). Additionally, *Bojjagani, Brabin & Rao (2020)* proposed a novel authentication protocol that sends a nonce message to a mobile customer device to avoid phishing attacks. DMARCBox provides analytical reports to combat email phishing, offering accurate graphical reports alongside geolocation mapping of email sources (*Nanaware, Mohite & Patil, 2019*). *Thakur & Yoshiura (2021)* propose AntiPhiMBS-Auth, a model for mobile banking systems, to combat phishing at the authentication level, addressing users who mistakenly download phishing apps and those vulnerable to phishing emails or SMS.

Other prevention methods. Other studies focus on specific aspects of phishing attacks. *Teerakanok, Yasuki & Uehara (2020)* presented a practical solution for detecting bogus invoice schemes using checksums from invoices and shared secret information. *Eshmawi & Nair (2019)* aimed to protect organizations from Smishing attacks with a roving proxy framework. *Goel, Sharma & Goswami (2017)* suggested a method to prevent QR code manipulation for sharing sensitive information. 'DeFD' distinguishes disguised executable files in phishing emails transferred over network connections to enhance incident response (*Ghafir et al., 2018*). Since phishing is the first step to initiating other attacks, *Lam & Kettani (2019)* focused on detecting and preventing ransomware delivery through phishing channels, while *Zhang et al. (2012)* introduced a VPN abuse detection system to identify compromised accounts rapidly. Virtual honeypot solutions are also used to prevent access to phishing sites (*Husák & Cegan, 2014*; *Chauhan & Shiwani, 2014*). *Ho et al. (2019)* developed a new detector for lateral phishing attacks to minimize false positives. Insider threat is one of the most common threats for lateral phishing, thus *He et al. (2024)* improved their phishing detection algorithm by utilizing Bi-LSTM with Attention mechanisms to detect insider threats based on user behavior. Since phishers nowadays start to encrypt their websites, *Ohmori (2023)* proposed a method to detect "Let's Encrypt" sites using TLS 1.2 or less as they easily provide free encryption certificates and are commonly used by attackers; however, such tools can be improved to accurately detect malicious websites.

Some solutions aim to protect a specific brand. For example, *Al-Hamar et al. (2021)* proposed a solution for specific organizations to defend against organization-targeted phishing emails, focusing on domain names, while *Ramanathan & Wechsler (2013)* proposed a multi-stage methodology to take down websites impersonating organizations.

These varied approaches underscore the multifaceted nature of phishing defense, highlighting the importance of interdisciplinary collaboration and technological innovation in combating evolving cyber threats.

Incident response

In response to the evolving landscape and sophistication of phishing threats (*Falowo et al., 2022*), numerous studies have investigated and developed mitigation strategies to combat phishing attacks and mitigate their damaging impacts.

Incident analysis and management. Incident analysis is an important step in the fight against phishing because organizations are required to mitigate the attack and learn from it to prevent future attacks. *Lacey, Salmon & Glancy (2015)* conducted a system analysis of processes, documentation, and activity logs to explore cyber situational awareness in organizations. To gain a deeper understanding of attack impact and the organizations' response, tools for analyzing and visualizing phishing attacks hitting the organizations have been developed to enhance cyber situational awareness of targeted phishing attacks (*Legg & Blackman, 2019*) and to assess security risks in banking institutions (*Gupta et al., 2021a*). Furthermore, *Gupta et al. (2021b)* developed a conceptual model to investigate social engineering attacks in a calculated way from several perspectives including attacker methods, exploit weaknesses, and the consequences of the attack on the cryptographic algorithms. Similarly, *Lohiya & Thakkar (2024)* reviewed several attack modeling techniques (*e.g.*, cyber kill chains, the diamond model, and security incident response matrix) for phishing attacks, revealing the significance of models to improve the risk assessment and response strategies. These tools and models help network defenders better understand the attacker's methodology, assess the risks at each attack stage, and implement timely mitigation strategies. Using a survey of professionals from major accounting firms in Nigeria, the research finds that digital forensic accounting significantly helps in reducing phishing scams, advance fee fraud, and credit card fraud (*Awodiran et al., 2023*).

Phishing reporting. Reporting phishing is essential in the fight against phishing because it allows organizations to respond quickly and block the attacks before they cause harm. To enhance the reporting rate, *Burda, Allodi & Zannone (2020)* proposed a crowd-sourced approach to automate response and containment against spear phishing, empowering users and strengthening resilience, which is observed by *Lain, Kostiainen & Čapkun (2022)* who found that employees can effectively and quickly report phishing emails while maintaining consistent reporting rate. Interestingly, while 31% of employees had the intention to report phishing emails, the most believable phishing emails are less likely to be reported compared to obvious ones (*Kersten et al., 2022*), making it important to raise awareness about the importance of reporting. Interestingly, this approach has shown to be successful in a small and medium-sized organization because of the strength of the community as employees are encouraged to share suspicious communications quickly, which can significantly enhance phishing resilience (*Burda et al., 2023*). For example, it can reduce the cost of advanced security plans by utilizing the human firewall system in detecting and preventing phishing attacks (*Shin et al., 2023*). *Althobaiti, Jenkins & Vaniea (2021)* conducted a case study on the phishing response procedures to understand how phishing reports are handled in a UK-based university and found that the number of reports can be unmanageable even though the percentage of reports is low compared to the size of the organization; therefore, *Althobaiti et al. (2023)* proposed a clustering approach that aims to group similar emails into campaigns for the IT teams to deal with them.

Learning from previous attacks. Current attacks were examined by several studies to help organizations learn from incidents to prevent future events.

Oest et al. (2018) explored the anti-phishing ecosystem through phishing kit analysis, seeking insights into countering evolving social engineering techniques employed by cybercriminals. Additionally, profiling phishing emails based on attack groups has assisted organizations in understanding attack motives and devising effective countermeasures (*Lee et al., 2021a*). Using clustering techniques, *Vargas et al. (2016)* investigated the registered attack on a financial US institution by grouping phishing websites based on their similarities to distinguish attacker groups. Their findings can be utilized to update the anti-phishing filters to prevent such tactics. Other studies examined the human factors that are exploited by attackers, such as the use of targeted phishing that increases the success rates in penetrating organizational defenses, as seen in Swedish organizations (*Holm et al., 2014*), a telecommunication organization (*Abdullah & Mohd, 2019*), a university, and a large international consultancy company (*Burda et al., 2020*). This was also observed by *Kotson & Schulz (2015)* who found that phishers send unique curriculum vitae (CV) attachments based on the target victims' profiles. Furthermore, the way the phishing attack was delivered plays a significant role, sometimes more than the content of the message itself (*Burda et al., 2020*). The source of an email is one of the tactics used to deceive victims; for instance, emails spoofing an information technology (IT) department have led to a higher percentage of compromised accounts in an Emirates university (*Mohebzada et al., 2012*) and Swedish organizations (*Holm et al., 2014*). Similarly, showing professionalism in emails or phone calls that spoof banks is one of the tactics as they resemble the messages that they usually receive from their banks (*Jansen & Leukfeldt, 2015*). This tendency was also observed with Jordanian students who click on links from seemingly familiar sources, such as friends or relatives (*Manasrah, Akour & Alsukhni, 2015*). While these tactics can combat phishing attacks, frequent analysis of attack messages and delivery methods is needed, as a recent study found a significant increase in attack sophistication from 2010 to 2023. For example, email topics are shifted from security-focused to campus life topics along with a reduction in spelling errors (*Morrow, 2024*).

Cognitive vulnerabilities such as authority, liking, scarcity, consistency, social proof, and reciprocity were also exploited by phishers (*Taib et al., 2019*; *De Bona & Paci, 2020*; *Williams, Hinds & Joinson, 2018*). However, these strategies do not always guarantee success as a phishing simulation in a multinational financial organization showed that while some users fell for authority-based lures, scarcity was perceived as the least credible tactic (*Taib et al., 2019*). Social proof is also a powerful tool, as people are more likely to trust a source that appears to be trusted by others (*Taib et al., 2019*). Social distance can also be exploited as the more individuals perceive similarity with the sender, the higher the trust and the greater the risk of data compromise (*Martin, Lee & Parmar, 2021*). *Van Der Heijden & Allodi (2019)* analyzed cognitive vulnerabilities in phishing attacks to prioritize remediation efforts based on vulnerability triggers, to predict users' behavior and effectively mitigate the impact of phishing campaigns whereas *Abroshan et al. (2021)* presented a phishing mitigation solution leveraging human behavior and emotional cues to identify high-risk

users and apply appropriate mitigation strategies. This system evolves to provide tailored protection, enabling organizations to effectively safeguard vulnerable users.

Attack notifications. After a successful build of a phishing detection system, *Pires & Borges (2023)* developed a phishing responder model that does at least one of the following to the detected phishing attack: reporting the website *via* email, notification post on a Telegram channel and automatic reporting to Google SafeBrowsing. Sending warning emails about ongoing attacks can have limited effect as a preventive measure. For example, despite receiving warning emails from the IT department, some individuals still fell victim to phishing attacks, as noted by *Mohebzada et al. (2012)* and *Holm et al. (2014)*. Similarly, management messaging does not appear to directly influence outcomes, as warning messages have not been observed to reduce the number of clicks in phishing simulations (*McElwee, Murphy & Shelton, 2018*). These findings suggest that alternative or supplementary strategies may be necessary to prevent phishing attacks and mitigate their impact on organizations effectively.

These diverse approaches underscore the multifaceted nature of responding to phishing attacks, highlighting the importance of integrating technological innovations with insights from human behavior and cognitive psychology to develop comprehensive anti-phishing strategies.

GAPS AND OPEN QUESTIONS

Frameworks have advantages and disadvantages

Our investigation revealed that organizations frequently rely on established frameworks for IT and security management. These frameworks are guidelines designed to help organizations identify problems and adapt the practices and procedures based on their needs. While these guidelines offer flexibility, their lack of specificity makes it challenging for organizations to adopt them successfully (*Stevens et al., 2022*). The organization's sector, size, and budget play a significant role in tailoring practices, sometimes making it almost impossible to implement the frameworks or policies. This gap highlights the need for additional research that focuses on identifying these challenges based on the mentioned factors and provides a list of recommendations with the pros and cons of each, allowing stakeholders to decide which recommendation to follow. Identifying these challenges can also help researchers to develop tool-based solutions that simplify adherence to the guidelines.

Phishing can still pass through

Our literature assessment reveals continuing gaps and unsolved concerns that potentially provide opportunities for phishers to exploit systems, despite significant efforts in research and practical interventions to prevent phishing emails. Due to the nature of phishing attacks, organizational phishing management requires a multi-layer defense system starting from preventing the attack to mitigating the impact of the harvested victims and learning from that incident. Although this research demonstrates the substantial progress made in preventative measures that incorporate human and technical variables,

it also identifies a notable lack of studies on post-attack strategies. Research indicates that companies frequently lack the resources necessary to quickly and efficiently react to phishing attacks, which highlights the critical need for further investigation into post-attack recovery and defense mechanisms (*Naqvi et al., 2023*) to ensure comprehensive protection against phishing threats; for example, developing tools that can remove phishing emails from users inboxes as a replacement for the ineffective attack notification messages or developing tools that can update the blocking filters immediately for ongoing attack. Furthermore, longitudinal studies tracking phishing incidents and organizational responses over time could offer valuable insights into evolving trends and effective countermeasures in organizations. Learning that attackers change their tactics frequently, invitation studies, whether longitudinal or not, can benefit from automating the studies to make it easy for organizations and researchers to repeat the investigation when needed. Unresolved phishing attacks can lead to other and more damaging security issues, such as lateral phishing, where emails are sent from legitimate accounts (*Ho et al., 2019*). Future research should not only be on reducing the negative impact of phishing that passes through but also on detecting and preventing other attacks and training employees to recognize them before falling victims (*Chitare, Coventry & Nicholson, 2023*).

Shift of common attack vectors

The literature examined in this study encompasses a diversity of phishing vectors, including Email (60 occurrences), websites (19), URLs (10), QR codes (1), social networks (1), mobile web apps (3), SMS (1), and telephone calls (1). Email is the most researched phishing vector, with URLs and websites coming in second and third. The frequency of these vectors emphasizes the importance of investigating how to protect against them and comprehending how vulnerable people are to their social engineering tactics, which seek to encourage activities such as opening links, downloading malicious files, or disclosing private information. Additionally, researchers have made attempts to increase user knowledge of these attack vectors.

Nonetheless, there has been a noticeable increase in mobile phone-based phishing attacks, known as vishing. Although attackers have historically preferred emails with embedded links (*Verizon, 2022*; *APWG, 2023*; *ProofPoint, 2023*) reported an increase in vishing attacks- 40% in 2023 as compared to 2022- emphasizing the need for more research on this evolved threat vector. For example, *Jansen & Leukfeldt (2015)* discovered that victims frequently consider telephone-based attacks to be authentic since attackers simply need only to seem trustworthy. Similarly, there is a rapid increase in QR-code-based phishing attacks that deliver malicious links or attachments (*ProofPoint, 2024*). Organizational-based studies that target QR-Codes are limited although this attack vector is particularly dangerous. It is impossible to recognize phishing just by looking at the QR Code itself.

More research is necessary to thoroughly examine the aforementioned attacks and create practical detection and mitigation techniques, given the dynamic nature of phishing attempts.

Impact of sectors on phishing management

In our literature review, we observed a significant number of studies that focus on specific sectors, with educational organizations being the most investigated (25 occurrences), followed by financial institutions (15 occurrences), and industry/manufacturing sectors (10 occurrences). The comparative analyses across these sectors shown by several studies revealed that different sectors exhibit varying levels of susceptibility to phishing attacks and implement diverse security measures.

Further research can explore how organizations develop and implement phishing management plans specific to their sector. For instance, studies could investigate the effectiveness of sector-specific phishing awareness training programs and the adoption of security measures tailored to the particular risks faced by each sector. Additionally, comparative studies across sectors could highlight the unique challenges and best practices in phishing prevention and mitigation strategies. Given that financial organizations are frequent targets of phishing attacks, in-depth investigations into the tactics and strategies employed by attackers targeting these sectors could provide valuable insights for improving organizational defenses.

Methodological barriers in phishing studies

Phishing simulation is one of the most utilized methodologies in phishing for testing users' awareness, training users, and understanding their susceptibility to phishing. However, there are ethical considerations surrounding the use of such exercises. Such studies require informed consent about the purpose and risks of the simulation and a safe strategy to deliver the attack to users (*Finn & Jakobsson, 2007b*; *Finn & Jakobsson, 2007a*).

In addition to ethical concerns, the procurement process of implementing phishing simulations often reveals hidden costs that are typically overlooked (*Brunken et al., 2023*). While much of the existing research focuses on measuring user behavior through click rates or other immediate reactions, it often neglects the significant time and effort required from various organizational stakeholders, including IT, legal, and HR departments. These hidden costs can be a barrier, particularly for smaller organizations, making the deployment of simulations more challenging than anticipated. Challenges such as stakeholder involvement, technical difficulties, and system integration create friction in the process, often hindering successful implementation.

Most of the research done on organizations is typically carried out with the assistance and collaboration of actual IT departments. This collaboration ensures that the experiments are conducted in a controlled and ethical manner while ensuring that appropriate safeguards are in place to protect employees and organizational assets and facilitate the experiment procedures. Further study of the collaboration between organizational stakeholders and researchers is essential for advancing research in the area and addressing the methodological barriers posed by hidden costs, procurement challenges, and simplistic evaluation methods.

Generative AI in organization-based phishing research

Generative AI (GenAI) models, such as ChatGPT, present both risks and opportunities in organizational phishing research. While GenAI tools are primarily designed to assist with

generating human-like text, attackers can exploit them to create sophisticated phishing emails that mimic legitimate communication styles, making detection difficult (*Gupta et al., 2023*). Attackers can use techniques such as reverse psychology to manipulate these models, bypassing ethical constraints and generating cyber threats, including phishing attacks and malware. This misuse of AI highlights the need for research directed at understanding the capabilities of chatbots and safeguarding solutions to prevent exploitation by adversaries.

However, GenAI tools can also be leveraged defensively to enhance security within organizations. These AI models can analyze large amounts of data to detect patterns and anomalies that indicate phishing attempts, providing early threat detection (*Shanthi, Sasi & Gouthaman, 2023*). Additionally, they can automate incident response processes, helping organizations respond more quickly to phishing attacks by reducing the manual workload on security teams. Tools powered by AI can also assist in vulnerability management by identifying and prioritizing weak points in the organization's systems that could be exploited by phishers. Despite these benefits, researchers should explore the possibility of utilizing chatbots in research while focusing on the challenges of combining this use such as data quality issues, model explainability, and potential bias (*Shanthi, Sasi & Gouthaman, 2023*).

LIMITATIONS

A potential limitation of our study is that we used several organization-equivalent keywords to identify relevant research that targets organizations. While this approach could have resulted in the omission of some papers, we minimized this risk by using keywords commonly found in recent studies and thoroughly searching for them in the title, abstract, and keywords sections. Additionally, the potential for bias in selecting and analyzing the literature is acknowledged, as is the possibility that our classification of some studies may differ from the author's original intent. To mitigate these concerns, we conducted multiple discussions and iterations throughout the analysis process, ensuring a more balanced and comprehensive review.

CONCLUSION

Phishing remains an evolving threat to organizations around the globe. Its effective defense requires extensive cybersecurity measures. Although prior work provided insightful interventions, analytical data, and patterns, a multi-layered strategy that addresses prevention, detection, and mitigation is required. Developing successful phishing prevention techniques will require ongoing cooperation and innovation. By filling up the gaps in the literature and expanding our knowledge on phishing, we can enhance organizational security and mitigate the impact of cyber threats.

APPENDIX. DIGITAL LIBRARIES QUERIES

Queries were executed on the 13th of April, 2022.

IEEE Xplore search query

((“All Metadata”:Phishing AND “All Metadata”:organisation) OR (“All Metadata”: Phishing AND “All Metadata”:organization) OR (“All Metadata”: Phishing AND “All Metadata”:Institution) OR (“All Metadata”: Phishing AND “All Metadata”:corporation) OR (“All Metadata”: Phishing AND “All Metadata”:enterprise) OR (“All Metadata”: Phishing AND “All Metadata”:workplace) OR (“All Metadata”: Phishing AND “All Metadata”:organisational) OR (“All Metadata”: Phishing AND “All Metadata”:organizational) OR (“All Metadata”: Phishing AND “All Metadata”:incident) (“All Metadata”:Phish AND “All Metadata”:organisation) OR (“All Metadata”: Phish AND “All Metadata”:organization) OR (“All Metadata”: Phish AND “All Metadata”:Institution) OR (“All Metadata”: Phish AND “All Metadata”:corporation) OR (“All Metadata”: Phish AND “All Metadata”:enterprise) OR (“All Metadata”: Phish AND “All Metadata”:workplace) OR (“All Metadata”: Phish AND “All Metadata”:organisational) OR (“All Metadata”: Phish AND “All Metadata”:organizational) OR (“All Metadata”: Phish AND “All Metadata”:incident))

ACM search query

[[Title: phishing] OR [Title: phish] OR [Abstract: phishing] OR [Abstract: phish] OR [Keywords: phishing] OR [Keywords: phish]] AND [[Title: organisation] OR [Title: organization] OR [Title: institution] OR [Title: cooperation] OR [Title: enterprise] OR [Title: incident] OR [Title: workplace] OR [Title: organisational] OR [Title: organizational] OR [Abstract: organisation] OR [Abstract: organization] OR [Abstract: institution] OR [Abstract: cooperation] OR [Abstract: enterprise] OR [Abstract: incident] OR [Abstract: workplace] OR [Abstract: organisational] OR [Abstract: organizational] OR [Keywords: organisation] OR [Keywords: organization] OR [Keywords: institution] OR [Keywords: cooperation] OR [Keywords: enterprise] OR [Keywords: incident] OR [Keywords: workplace] OR [Keywords: organisational] OR [Keywords: organizational]]

ScienceDirect.com search query

title, abstract, keywords: ((phishing OR Phish) AND (organisation OR orgranization OR Institution OR cooperation OR Enterprise OR incident OR workplace OR organisational OR organizational OR Incident))

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

This work was funded by the Deanship of Scientific Research, Taif University. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Grant Disclosures

The following grant information was disclosed by the authors:
The Deanship of Scientific Research, Taif University.

Competing Interests

The authors declare there are no competing interests.

Author Contributions

- Kholoud Althobaiti conceived and designed the experiments, performed the experiments, analyzed the data, authored or reviewed drafts of the article, and approved the final draft.
- Nawal Alsufyani conceived and designed the experiments, performed the experiments, analyzed the data, authored or reviewed drafts of the article, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

This is a literature review.

REFERENCES

Abawajy JH. 2014. User preference of cyber security awareness delivery methods. *Behaviour and Information Technology* **33(3)**:236–247 DOI 10.1080/0144929X.2012.708787.

Abdullah AS, Mohd M. 2019. Spear phishing simulation in critical sector: telecommunication and defense sub-sector. In: *International conference on cybersecurity (ICoCSec)*. 26–31 DOI 10.1109/ICoCSec47621.2019.8970803.

Abroshan H, Devos J, Poels G, Laermans E. 2021. A phishing mitigation solution using human behaviour and emotions that influence the success of phishing attacks. In: *Adjunct proceedings of the 29th ACM conference on user modeling, adaptation and personalization*. New York, NY, USA: Association for Computing Machinery, 345–350.

Al-hamar Y, Kolivand H. 2020. A new email phishing training website. In: *13th international conference on developments in eSystems engineering (DeSE)*. 263–268 DOI 10.1109/DeSE51703.2020.9450238.

Al-Hamar Y, Kolivand H, Tajdini M, Saba T, Ramachandran V. 2021. Enterprise credential spear-phishing attack detection. *Computers & Electrical Engineering* **94**:1–25 DOI 10.1016/j.compeleceng.2021.107363.

Alabdan R. 2020. Phishing attacks survey: types, vectors, and technical approaches. *Future Internet* **12(10)**:1–39 DOI 10.3390/fi12100168.

Aldawood H, Skinner G. 2018. Educating and raising awareness on cyber security social engineering: a literature review. In: *IEEE international conference on teaching, assessment, and learning for engineering (TALE)*. Piscataway: IEEE, 62–68 DOI 10.1109/TALE.2018.8615162.

Aleroud A, Abu-Shanab E, Al-Aiad A, Alshboul Y. 2020. An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities. *Journal of Information Security and Applications* **55**:1–15 DOI 10.1016/j.jisa.2020.102614.

AlEroud A, Zhou L. 2017. Phishing environments, techniques, and countermeasures: a survey. *Computers and Security* **68**:160–196 DOI 10.1016/j.cose.2017.04.006.

Alizadeh F, Stevens G, Jakobi T, Krüger J. 2023. Catch Me if You Can: "Delaying" as a social engineering technique in the post-attack phase. In: *Proceedings of the ACM on Human-Computer Interactions. CSCW1, vol. 7*. New York: ACM, 1–25 DOI 10.1145/3579465.

Alkhazi B, Alshaikh M, Alkhezi S, Labbaci H. 2022. Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior. *IEEE Access* **10**:132132–132143 DOI 10.1109/ACCESS.2022.3230286.

Alsubaei FS, Almazroi AA, Ayub N. 2024. Enhancing phishing detection: a novel hybrid deep learning framework for cybercrime forensics. *IEEE Access* **12**:8373–8389 DOI 10.1109/ACCESS.2024.3351946.

Althobaiti K, Jenkins ADG, Vaniea K. 2021. A case study of phishing incident response in an educational organization. *Proceedings of the ACM on Human Computer Interaction* **5**:338 DOI 10.1145/3476079.

Althobaiti K, Wolters MK, Alsufyani N, Vaniea K. 2023. Using clustering algorithms to automatically identify phishing campaigns. *IEEE Access* **11**:96502–96513 DOI 10.1109/ACCESS.2023.3310810.

Andrić J, Oreški D, Kišasondi T. 2016. Analysis of phishing attacks against students. In: *2016 39th international convention on information and communication technology, electronics and microelectronics (MIPRO)*. 1423–1429 DOI 10.1109/MIPRO.2016.7522363.

APWG. 2023. Phishing activity trends report, 1st quarter 2023. Technical report. Anti-Phishing Working Group. *Available at https://docs.apwg.org/reports/apwg_trends_report_q1_2023.pdf* .

Arachchilage NAG, Cole M. 2016. Designing a mobile game for home computer users to protect against phishing attacks. DOI 10.1109/i-Society18435.2011.5978543.

Arachchilage NAG, Love S, Maple C. 2015. Can a mobile game teach computer users to thwart phishing attacks? DOI 10.20533/iji.1742.4712.2013.0083.

Aslam S, Nassif AB. 2023. Phish-identifier: machine Learning based classification of Phishing attacks. In: *2023 advances in science and engineering technology international conferences (ASET)*. 1–6 DOI 10.1109/ASET56582.2023.10180869.

Awodiran MA, Ogundele AT, Idem UJ, Anwana , Emem O. 2023. Digital forensic accounting and cyber fraud in Nigeria. In: *2023 international conference on cyber management and engineering (CyMaEn)*. 321–326 DOI 10.1109/CyMaEn57228.2023.10050992.

Bakar NA, Mohd M, Sulaiman R. 2017. Information leakage preventive training. In: *2017 6th international conference on electrical engineering and informatics (ICEEI)*. 1–6 DOI 10.1109/ICEEI.2017.8312403.

Bakhshi T. 2017. Social engineering: revisiting end-user awareness and susceptibility to classic attack vectors. In: *2017 13th international conference on emerging technologies (ICET)*. 1–6 DOI 10.1109/ICET.2017.8281653.

Bann LL, Singh MM, Samsudin A. 2015. Trusted security policies for tackling advanced persistent threat via spear phishing in BYOD environment. *Procedia Computer Science* **72**:129–136 DOI 10.1016/j.procs.2015.12.113.

Benenson Z, Gassmann F, Landwirth R. 2017. Unpacking spear phishing susceptibility. In: *Financial cryptography and data security—fc international workshops, malta revised selected papers, vol. 10323. Lecture notes in computer science*. Cham: Springer, 610–627 DOI 10.1007/978-3-319-70278-0_39.

Bhurtel M, Siwakoti YR, Rawat DB. 2022. Phishing attack detection with ML-based siamese empowered ORB logo recognition and IP mapper. In: *IEEE INFOCOM 2022—IEEE conference on computer communications workshops (INFOCOM WKSHPS)*. Piscataway: IEEE, 1–6 DOI 10.1109/INFOCOMWKSHPS54753.2022.9798203.

Birajdar A, Nisha TN. 2022. APPEARS framework for evaluating gamified cyber security awareness training. In: *2022 international conference on computing, communication, security and intelligent systems (IC3SIS)*. 1–8 DOI 10.1109/IC3SIS54991.2022.9885399.

Blancaflor E, Banzon CVH, Jackson CJJ, Jamena JN, Miraflores J, Samala LK. 2021. Risk assessments of social engineering attacks and set controls in an online education environment. In: *3rd international conference on modern educational technology, ICMET 2021*. New York, NY, USA: Association for Computing Machinery, 69–74 DOI 10.1145/3468978.3468990.

Blythe JM, Gray A, Collins E. 2020. Human cyber risk management by security awareness professionals: carrots or sticks to drive behaviour change? In: *HCI for cybersecurity, privacy and trust: second international conference, HCI-CPT 2020, held as Part of the 22nd HCI international conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 76–91 DOI 10.1007/978-3-030-50309-3_6.

Bojjagani S, Brabin DRD, Rao PVV. 2020. PhishPreventer: a secure authentication protocol for prevention of phishing attacks in mobile environment with formal verification. *Procedia Computer Science* **171**:1110–1119 DOI 10.1016/j.procs.2020.04.119.

Bouijij H, Berqia A, Saliah-Hassan H. 2022. Phishing URL classification using extra-tree and DNN. In: *2022 10th international symposium on digital forensics and security (ISDFS)*. 1–6 DOI 10.1109/ISDFS55398.2022.9800795.

Brunken L, Buckmann A, Hielscher J, Sasse MA. 2023. "To Do This Properly, You Need More Resources": the hidden costs of introducing simulated phishing campaigns. In: *32nd USENIX security symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, 4105–4122.

Buckley J, Lottridge D, Murphy J, Corballis P. 2023. Indicators of employee phishing email behaviours: Intuition, elaboration, attention, and email typology. *International Journal of Human-Computer Studies* **172**:102996 DOI 10.1016/j.ijhcs.2023.102996.

Burda P, Allodi L, Zannone N. 2020. Don't forget the human: a crowdsourced approach to automate response and containment against spear phishing attacks.

In: *IEEE European symposium on security and privacy workshops, EuroS&P workshops 2020, Genoa, Italy, September 7–11, 2020*. Piscataway: IEEE, 471–476 DOI 10.1109/EUROSPW51379.2020.00069.

Burda P, Altawekji AM, Allodi L, Zannone N. 2023. The peculiar case of tailored phishing against SMEs: detection and collective defense mechanisms at a small IT company. In: *2023 IEEE European symposium on security and privacy workshops (EuroS&PW)*. Piscataway: IEEE, 232–243 DOI 10.1109/EuroSPW59978.2023.00031.

Burda P, Chotza T, Allodi L, Zannone N. 2020. Testing the effectiveness of tailored phishing techniques in industry and academia: a field experiment. In: *Proceedings of the 15th international conference on availability, reliability and security, ARES '20*. New York, NY, USA: Association for Computing Machinery, DOI 10.1145/3407023.3409178.

Bursztein E, Benko B, Margolis D, Pietraszek T, Archer A, Aquino A, Pitsillidis A, Savage S. 2014. Handcrafted fraud and extortion: manual account hijacking in the wild. In: *Internet measurement conference, IMC, Vancouver, BC, Canada, November 5–7*. ACM, 347–358 DOI 10.1145/2663716.2663749.

Calvo A, Escuder S, Escrig J, Arias M, Ortiz N, Guijarro J. 2023. A data-driven approach for risk exposure analysis in enterprise security. In: *2023 IEEE 10th international conference on data science and advanced analytics (DSAA)*. Piscataway: IEEE, 1–9 DOI 10.1109/DSAA60987.2023.10302480.

Chauhan S, Shiwani S. 2014. A honeypots based anti-phishing framework. In: *2014 international conference on control, instrumentation, communication and computational technologies (ICCICCT)*. 618–625 DOI 10.1109/ICCICCT.2014.6993036.

Chen Y, Zahedi FM, Abbasi A, Dobolyi D. 2021. Trust calibration of automated security IT artifacts: a multi-domain study of phishing-website detection tools. *Information & Management* **58(1)**:103394 DOI 10.1016/j.im.2020.103394.

Chin T, Xiong K, Hu C. 2018. Phishlimiter: a phishing detection and mitigation approach using software-defined networking. *IEEE Access* **6**:42516–42531 DOI 10.1109/ACCESS.2018.2837889.

Chitare N, Coventry L, Nicholson J. 2023. "It may take ages": understanding human-centred lateral phishing attack detection in organisations. In: *Proceedings of the 2023 European Symposium on Usable Security, vol. EuroUSEC '23*. New York, NY, USA: Association for Computing Machinery, 344–355 DOI 10.1145/3617072.3617116.

Clark JW. 2012. Everything but the kitchen sink: determining the effect of multiple attacks on privacy preserving technology users. In: *Proceedings of the 17th Nordic conference on secure IT systems, NordSec'12*. Berlin, Heidelberg: Springer-Verlag, 199–214 DOI 10.1007/978-3-642-34210-3_14.

Cofense. 2023. Annual state of email secuirty report. Technical report. Cofense Email Security. *Available at https://cofense.com/annualreport*.

Conway D, Taib R, Harris M, Berkovsky S, Yu K, Chen F. 2017. A qualitative investigation of bank employee experiences of information security and phishing. In: *Proceedings of the thirteenth USENIX conference on usable privacy and security, SOUPS '17*. USENIX Association, USA, 115–129.

Coronges K, Dodge R, Mukina C, Radwick Z, Shevchik J, Rovira E. 2012. The influences of social networks on phishing vulnerability. In: *Proceedings of the 2012 45th Hawaii international conference on system sciences, HICSS '12*. Piscataway: IEEE, 2366–2373 DOI 10.1109/HICSS.2012.657.

Cuchta T, Blackwood B, Devine TR, Niichel RJ, Daniels KM, Lutjens CH, Maibach S, Stephenson RJ. 2019. Human risk factors in cybersecurity. In: *Proceedings of the 20th annual SIG conference on information technology education, SIGITE '19*. New York, NY, USA: Association for Computing Machinery, 87–92 DOI 10.1145/3349266.3351407.

Cuzzocrea A, Martinelli F, Mercaldo F. 2018. Applying machine learning techniques to detect and analyze web phishing attacks. In: *Proceedings of the 20th international conference on information integration and web-based applications & services*. New York, NY, USA: Association for Computing Machinery, 355–359 DOI 10.1145/3282373.3282422.

Daengsi T, Wuttidittachotti P, Pornpongtechavanich P, Utakrit N. 2021. A comparative study of cybersecurity awareness on phishing among employees from different departments in an organization. In: *2nd international conference on smart computing and electronic enterprise (ICSCEE)*. 102–106 DOI 10.1109/ICSCEE50312.2021.9498208.

Darwish A, Zarka AE, Aloul F. 2012. Towards understanding phishing victims' profile. In: *2012 international conference on computer systems and industrial informatics*. 1–5 DOI 10.1109/ICCSII.2012.6454454.

De Bona M, Paci F. 2020. A real world study on employees' susceptibility to phishing attacks. In: *Proceedings of the 15th international conference on availability, reliability and security, ARES '20*. New York, NY, USA: Association for Computing Machinery, DOI 10.1145/3407023.3409179.

Desolda G, Ferro LS, Marrella A, Catarci T, Costabile MF. 2021. Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)* **54(8)**:1–35.

Deval SK, Tripathi M, Bezawada B, Ray I. 2021. "X-Phish: days of future past"‡: adaptive amp; privacy preserving phishing detection. In: *IEEE conference on communications and network security (CNS)*. Piscataway: IEEE, 227–235 DOI 10.1109/CNS53000.2021.9705052.

Devalla V, Srinivasa Raghavan S, Maste S, Kotian JD, Annapurna DD. 2022. mURLi: a tool for detection of malicious URLs and injection attacks. In: *4th international conference on innovative data communication technology and application, vol. 215*. 662–676 DOI 10.1016/j.procs.2022.12.068.

Dewan P, Kashyap A, Kumaraguru P. 2014. Analyzing social and stylometric features to identify spear phishing emails. In: *2014 APWG symposium on electronic crime research (eCrime)*. 1–13 DOI 10.1109/ECRIME.2014.6963160.

Dixit P, Silakari S. 2021. Deep learning algorithms for cybersecurity applications: a technological and status review. *Computer Science Review* **39**:100317 DOI 10.1016/j.cosrev.2020.100317.

Dolnák I, Kampová K. 2022. BIMI specification as another technical approach in the fight against e-mail phishing. In: *2022 20th international conference on emerging elearning technologies and applications (ICETA)*. 129–134 DOI 10.1109/ICETA57911.2022.9974949.

Dubey S, Singh P, Verma RK, Kamboj D. 2023. Government tender allocation using blockchain technology. In: *2023 international conference on IoT, communication and automation technology (ICICAT)*. 1–6 DOI 10.1109/ICICAT57735.2023.10263653.

Dunđer I, Seljan S, Odak M. 2023. Data acquisition and corpus creation for phishing detection. In: *2023 46th MIPRO ICT and electronics convention (MIPRO)*. 533–538 DOI 10.23919/MIPRO57284.2023.10159904.

Eftimie S, Cotenescu V, Moinescu R, Răcuciu C, Glăvan D. 2021. A case study in anticipating insider vulnerabilities using psychological profiling. In: *IEEE international black sea conference on communications and networking (BlackSeaCom)*. Piscataway: IEEE, 1–4 DOI 10.1109/BlackSeaCom52164.2021.9527896.

Eshmawi A, Nair S. 2019. The roving proxy framewrok for SMS spam and phishing detection. In: *2nd international conference on computer applications information security (ICCAIS)*. 1–6 DOI 10.1109/CAIS.2019.8769562.

Falowo OI, Popoola S, Riep J, Adewopo VA, Koch J. 2022. Threat actors' tenacity to disrupt: examination of major cybersecurity incidents. *IEEE Access* **10**:134038–134051 DOI 10.1109/ACCESS.2022.3231847.

Finn P, Jakobsson M. 2007a. Designing and conducting phishing experiments. In: *IEEE technology and society magazine, special issue on usability and security*. Piscataway: IEEE.

Finn P, Jakobsson M. 2007b. Designing ethical phishing experiments. *IEEE Technology and Society Magazine* **26(1)**:46–58 DOI 10.1109/MTAS.2007.335565.

Flores P, Farid M, Samara K. 2019. Assessing E-security behavior among students in higher education. In: *Sixth HCT information technology trends (ITT)*. 253–258 DOI 10.1109/ITT48889.2019.9075100.

Flores WR, Holm H, Ekstedt M, Nohlberg M. 2015. Investigating the correlation between intention and action in the context of social engineering in two different national cultures. In: *Proceedings of the 2015 48th Hawaii international conference on system sciences, HICSS '15*. Piscataway: IEEE, 3508–3517 DOI 10.1109/HICSS.2015.422.

Franz A, Zimmermann V, Albrecht G, Hartwig K, Reuter C, Benlian A, Vogt J. 2021. SoK: still plenty of phish in the Sea—a taxonomy of user-oriented phishing interventions and avenues for future research. In: *Seventeenth symposium on usable privacy and security (SOUPS 2021)*. 339–358.

Frauenstein ED, Von Solms R. 2009. Phishing: how an organization can protect itself. In: *Information security South Africa conference 2009, School of Tourism & Hospitality, Proceedings ISSA2009*. Johannesburg, South Africa: University of Johannesburg, ISSA, Pretoria, South Africa, 253–268.

Frauenstein ED, Von Solms R. 2013. An enterprise anti-phishing framework. In: *Information assurance and security education and training—8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Proceedings, IFIP Advances*

in Information and Communication Technology, vol. 406. Auckland, New Zealand: Springer, 196–203 DOI 10.1007/978-3-642-39377-8_22.

Frauenstein ED, Von Solms R. 2014. Combatting phishing: a holistic human approach. In: *2014 information security for South Africa*. 1–10 DOI 10.1109/ISSA.2014.6950508.

Gangavarapu T, Jaidhar C, Chanduka B. 2020. Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review* **53**:5019–5081 DOI 10.1007/s10462-020-09814-9.

Ghafir I, Prenosil V, Hammoudeh M, Aparicio-Navarro FJ, Rabie K, Jabban A. 2018. Disguised executable files in spear-phishing emails: detecting the point of entry in advanced persistent threat. In: *Proceedings of the 2nd international conference on future networks and distributed systems, vol. ICFNDS '18*. New York, NY, USA: Association for Computing Machinery, DOI 10.1145/3231053.3231097.

Goel D, Jain AK. 2018. Mobile phishing attacks and defence mechanisms: state of art and open research challenges. *Computers & Security* **73**:519–544 DOI 10.1016/j.cose.2017.12.006.

Goel N, Sharma A, Goswami S. 2017. A way to secure a QR code: SQR. In: *2017 international conference on computing, communication and automation (ICCCA)*. 494–497 DOI 10.1109/CCAA.2017.8229850.

Gupta A, Sharma V, Pragya , Srivastava R. 2021a. BISRAC banking information security risk assessment and compliance model. In: *3rd international conference on advances in computing, communication control and networking (ICAC3N)*. 1447–1452 DOI 10.1109/ICAC3N53548.2021.9725576.

Gupta BB, Arachchilage NAG, Psannis KE. 2018. Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems* **67(2)**:247–267 DOI 10.1007/s11235-017-0334-z.

Gupta BB, Tewari A, Jain AK, Agrawal DP. 2017. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications* **28(12)**:3629–3654 DOI 10.1007/s00521-016-2275-y.

Gupta M, Akiri C, Aryal K, Parker E, Praharaj L. 2023. From ChatGPT to ThreatGPT: impact of generative AI in cybersecurity and privacy. *IEEE Access* **11**:80218–80245 DOI 10.1109/ACCESS.2023.3300381.

Gupta S, Gupta MP, Chaturvedi M, Vilkhu MS, Kulshrestha S, Gaurav D, Mittal A. 2020. Guess who?—A serious game for cybersecurity professionals. In: *Games and learning alliance: 9th international conference, GALA 2020, Laval, France, December 9–10, 2020, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 421–427 DOI 10.1007/978-3-030-63464-3_41.

Gupta S, Isha , Bhattacharya A, Gupta H. 2021b. Analysis of social engineering attack on cryptographic algorithm. In: *9th international conference on reliability, infocom technologies and optimization (Trends and Future Directions) (ICRITO)*. 1–5 DOI 10.1109/ICRITO51393.2021.9596568.

Hajgude J, Ragha L. 2012. Phish mail guard: phishing mail detection technique by using textual and URL analysis. In: *2012 world congress on information and communication technologies*. 297–302 DOI 10.1109/WICT.2012.6409092.

Hammour RA, Gharaibeh YA, Qasaimeh M, Al-Qassas RS. 2019. The status of information security systems in banking sector from social engineering perspective. In: *Proceedings of the second international conference on data science, E-learning and information systems, DATA '19*. New York, NY, USA: Association for Computing Machinery, DOI 10.1145/3368691.3368705.

He D, Lv X, Xu X, Chan S, Choo K-KR. 2024. Double-layer detection of internal threat in enterprise systems based on deep learning. *IEEE Transactions on Information Forensics and Security* **19**:4741–4751 DOI 10.1109/TIFS.2024.3372771.

Hermogenes MGG, Capariño ET. 2019. Evaluating internet security awareness and practices of BulSU-SC students. In: *Proceedings of the 2019 7th international conference on information and education technology, ICIET 2019*. New York, NY, USA: Association for Computing Machinery, 62–66 DOI 10.1145/3323771.3323780.

Higashino M. 2019. A design of an anti-phishing training system collaborated with multiple organizations. In: *Proceedings of the 21st international conference on information integration and web-based applications & services, iiWAS 2019, December 2–4, 2019*. Munich, Germany: ACM, 589–592 DOI 10.1145/3366030.3366086.

Higashino M, Kawato T, Ohmori M, Kawamura T. 2019. An anti-phishing training system for security awareness and education considering prevention of information leakage. In: *5th international conference on information management (ICIM)*. 82–86 DOI 10.1109/INFOMAN.2019.8714691.

Hillman D, Harel Y, Toch E. 2023. Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security* **132**:1–17 DOI 10.1016/j.cose.2023.103364.

Ho G, Cidon A, Gavish L, Schweighauser M, Paxson V, Savage S, Voelker GM, Wagner D. 2019. Detecting and characterizing lateral phishing at scale. In: *Proceedings of the 28th USENIX conference on security symposium, SEC'19*. Berkeley: USENIX Association, 1273–1290.

Holm H, Flores WR, Nohlberg M, Ekstedt M. 2014. An empirical investigation of the effect of target-related information in phishing attacks. In: *IEEE 18th international enterprise distributed object computing conference workshops and demonstrations*. Piscataway: IEEE, 357–363 DOI 10.1109/EDOCW.2014.59.

Hu H, Peng P, Wang G. 2018. Towards understanding the adoption of anti-spoofing protocols in email systems. In: *IEEE cybersecurity development (SecDev)*. 94–101 DOI 10.1109/SecDev.2018.00020.

Husák M, Cegan J. 2014. PhiGARo: automatic phishing detection and incident response framework. In: *2014 ninth international conference on availability, reliability and security*. 295–302 DOI 10.1109/ARES.2014.46.

Ikhsan MG, Ramli K. 2019. Measuring the information security awareness level of government employees through phishing assessment. In: *34th international technical conference on circuits/systems, computers and communications (ITC-CSCC)*. 1–4 DOI 10.1109/ITC-CSCC.2019.8793292.

Innab N, Al-Rashoud H, Al-Mahawes R, Al-Shehri W. 2018. Evaluation of the effective anti-phishing awareness and training in governmental and private organizations in

Riyadh. In: *21st Saudi computer society national computer conference (NCC)*. 1–5 DOI 10.1109/NCG.2018.8593144.

Ismail KA, Singh MM, Mustaffa N, Keikhosrokiani P, Zulkefli Z. 2017. Security strategies for hindering watering hole cyber crime attack. *Procedia Computer Science* **124**:656–663 DOI 10.1016/j.procs.2017.12.202.

Itani D, Itani R, Eltweri AA, Faccia A, Wanganoo L. 2024. Enhancing cybersecurity through compliance and auditing: a strategic approach to resilience. In: *2024 2nd international conference on cyber resilience (ICCR)*. 1–10 DOI 10.1109/ICCR61006.2024.10532959.

Ito D, Takata Y, Kamizono M. 2022. Money talks: detection of disposable phishing websites by analyzing its building costs. In: *2022 IEEE 4th international conference on trust, privacy and security in intelligent systems, and applications (TPS-ISA)*. Piscataway: IEEE, 97–106 DOI 10.1109/TPS-ISA56441.2022.00022.

Jain AK, Gupta BB. 2016. A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal Information Security* **2016**:1–11 DOI 10.1186/s13635-016-0034-3.

Jampen D, Gür G, Sutter T, Tellenbach B. 2020. Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences* **10(1)**:1–41 DOI 10.1186/s13673-019-0205-6.

Jansen J, Leukfeldt R. 2015. How people help fraudsters steal their money: an analysis of 600 online banking fraud cases. In: *Proceedings of the 2015 workshop on socio-technical aspects in security and trust, STAST '15*. Piscataway: IEEE, 24–31 DOI 10.1109/STAST.2015.12.

Kearney W, Kruger H. 2014. Considering the influence of human trust in practical social engineering exercises. In: *2014 information security for South Africa*. 1–6 DOI 10.1109/ISSA.2014.6950509.

Kepkowski M, Machulak M, Wood I, Kaafar D. 2023. Challenges with passwordless FIDO2 in an enterprise setting: a usability study. In: *2023 IEEE secure development conference (SecDev)*. 37–48 DOI 10.1109/SecDev56634.2023.00017.

Kersten L, Burda P, Allodi L, Zannone N. 2022. Investigating the effect of phishing believability on phishing reporting. In: *2022 IEEE european symposium on security and privacy workshops (EuroS&PW)*. 117–128 DOI 10.1109/EuroSPW55150.2022.00018.

Kokulu FB, Soneji A, Bao T, Shoshitaishvili Y, Zhao Z, Doupé A, Ahn G. 2019. Matched and mismatched SOCs: a qualitative study on security operations center issues. In: *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, CCS*. London, UK: ACM, 1955–1970 DOI 10.1145/3319535.3354239.

Kotson MC, Schulz A. 2015. Characterizing phishing threats with Natural Language Processing. In: *IEEE conference on communications and network security (CNS)*. Piscataway: IEEE, 308–316 DOI 10.1109/CNS.2015.7346841.

Kulkarni M, Kumar S, Panjwani Y, Mohana , Moharir M, Ashok Kumar AR, Baskaran E. 2024. Mitigating email phishing: analytical framework, simulation models, and preventive measures. In: *2024 10th international conference on communication and signal processing (ICCSP)*. 1459–1464 DOI 10.1109/ICCSP60870.2024.10543325.

Lacey D, Salmon P, Glancy P. 2015. Taking the bait: a systems analysis of phishing attacks. *Procedia Manufacturing* **3**:1109–1116 DOI 10.1016/j.promfg.2015.07.185.

Lain D, Kostiainen K, Čapkun S. 2022. Phishing in organizations: findings from a large-scale and long-term study. In: *2022 IEEE symposium on security and privacy (SP)*. Piscataway: IEEE, 842–859 DOI 10.1109/SP46214.2022.9833766.

Lam T, Kettani H. 2019. PhAttApp: a phishing attack detection application. In: *Proceedings of the 2019 3rd international conference on information system and data mining, ICISDM 2019*. New York, NY, USA: Association for Computing Machinery, 154–158 DOI 10.1145/3325917.3325927.

Lee J, Lee Y, Lee D, Kwon H, Shin D. 2021a. Classification of attack types and analysis of attack methods for profiling phishing mail attack groups. *IEEE Access* **9**:80866–80872 DOI 10.1109/ACCESS.2021.3084897.

Lee J, Tang F, Ye P, Abbasi F, Hay P, Divakaran DM. 2021b. D-Fence: a flexible, efficient, and comprehensive phishing email detection system. In: *IEEE European symposium on security and privacy (EuroS P)*. Piscataway: IEEE, 578–597 DOI 10.1109/EuroSP51992.2021.00045.

Legg P, Blackman T. 2019. Tools and techniques for improving cyber situational awareness of targeted phishing attacks. In: *International conference on cyber situational awareness, data analytics and assessment (Cyber SA)*. 1–4 DOI 10.1109/CyberSA.2019.8899406.

Liu Y, Zhang M. 2012. Financial websites oriented heuristic anti-phishing research. In: *IEEE 2nd international conference on cloud computing and intelligence systems, vol. 02*. Piscataway: IEEE, 614–618 DOI 10.1109/CCIS.2012.6664247.

Lohiya R, Thakkar A. 2024. A compendium on risk assessment of phishing attack using attack modeling techniques. *Procedia Computer Science* **235**:1105–1114. International Conference on Machine Learning and Data Engineering (ICMLDE 2023) DOI 10.1016/j.procs.2024.04.105.

Madleňák M, Kampová K. 2022. Phishing as a cyber security threat. In: *2022 20th international conference on emerging elearning technologies and applications (ICETA)*. 392–396 DOI 10.1109/ICETA57911.2022.9974817.

Mahbub S, Pardede E, Kayes ASM. 2022. Online recruitment fraud detection: a study on contextual features in australian job industries. *IEEE Access* **10**:82776–82787 DOI 10.1109/ACCESS.2022.3197225.

Manasrah A, Akour M, Alsukhni E. 2015. Toward improving university students awareness of spam email and cybercrime: case study of Jordan. In: *2015 first international conference on anti-cybercrime (ICACC)*. 1–6 DOI 10.1109/Anti-Cybercrime.2015.7351955.

Martin SR, Lee JJ, Parmar BL. 2021. Social distance, trust and getting "hooked": a phishing expedition. *Organizational Behavior and Human Decision Processes* **166**:39–48 DOI 10.1016/j.obhdp.2019.08.001.

Mathew AR, Al Hajj A, Al Ruqeishi K. 2010. Cyber crimes: threats and protection. In: *2010 international conference on networking and information technology*. 16–18 DOI 10.1109/ICNIT.2010.5508568.

Matovu R, Nwokeji JC, Holmes T, Rahman T. 2022. Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges. In: *2022 IEEE frontiers in education conference (FIE)*. Piscataway: IEEE, 1–9 DOI 10.1109/FIE56618.2022.9962519.

McElwee S, Murphy G, Shelton P. 2018. Influencing outcomes and behaviors in simulated phishing exercises. In: *SoutheastCon 2018*. 1–6 DOI 10.1109/SECON.2018.8479109.

Meyers JJ, Hansen DL, Giboney JS, Rowe DC. 2018. Training future cybersecurity professionals in spear phishing using SiEVE. In: *Proceedings of the 19th annual SIG conference on information technology education, SIGITE '18*. New York, NY, USA: Association for Computing Machinery, 135–140 DOI 10.1145/3241815.3241871.

Miyamoto D, Iimura T, Blanc G, Tazaki H, Kadobayashi Y. 2014. EyeBit: eye-tracking approach for enforcing phishing prevention habits. In: *2014 third international workshop on building analysis datasets and gathering experience returns for security (BADGERS)*. 56–65 DOI 10.1109/BADGERS.2014.14.

Mohebzada JG, Zarka AE, Bhojani AH, Darwish A. 2012. Phishing in a university community: two large scale phishing experiments. In: *2012 international conference on innovations in information technology (IIT)*. 249–254 DOI 10.1109/INNOVATIONS.2012.6207742.

Morrow E. 2024. Scamming higher ed: an analysis of phishing content and trends. *Computers in Human Behavior* **158**:1–10 DOI 10.1016/j.chb.2024.108274.

Mossano M, Vaniea K, Aldag L, Düzgün R, Mayer P, Volkamer M. 2020. Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector. In: *European symposium on security and privacy workshops, EuroS&P Workshops*. Piscataway: IEEE, 130–139 DOI 10.1109/EuroSPW51379.2020.00026.

Moul KA. 2019. Avoid phishing traps. In: *ACM SIGUCCS annual conference, SIGUCCS*. New York: ACM, 199–208 DOI 10.1145/3347709.3347774.

Mouton F, Leenen L, Venter HS. 2016. Social engineering attack examples, templates and scenarios. *Computers & Security* **59**:186–209 DOI 10.1016/j.cose.2016.03.004.

Mouton F, Malan MM, Leenen L, Venter HS. 2014. Social engineering attack framework. In: *2014 information security for South Africa*. 1–9.

Muneer A, Ali RF, Al-Sharai AA, Fati SM. 2021. A survey on phishing emails detection techniques. In: *International conference on innovative computing (ICIC)*. 1–6 DOI 10.1109/ICIC53490.2021.9692960.

Nanaware T, Mohite P, Patil R. 2019. DMARCBox—corporate email security and analytics using DMARC. In: *IEEE 5th international conference for convergence in technology (I2CT)*. Piscataway: IEEE, 1–5 DOI 10.1109/I2CT45611.2019.9033552.

Naqvi B, Perova K, Farooq A, Makhdoom I, Oyedeji S, Porras J. 2023. Mitigation strategies against the phishing attacks: a systematic literature review. *Computers & Security* **132**:1–25 DOI 10.1016/J.COSE.2023.103387.

Nicholson J, Coventry L, Briggs P. 2017. Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection. In: *Proceedings of the thirteenth USENIX conference on usable privacy and security, SOUPS '17*. USA: USENIX Association, 285–298.

Niroshan Atimorathanna D, Shehan Ranaweera T, Devdunie Pabasara R, Rukshila Perera J, Yapa Abeywardena K. 2020. NoFish; Total anti-phishing protection system. In: *2nd International Conference on Advancements in Computing (ICAC), vol. 1*. 470–475 DOI 10.1109/ICAC51239.2020.9357145.

NSCS. 2018. Phishing attacks: defending your organisation. NCSC guidance. National Cyber Security Centre. *Available at https://www.ncsc.gov.uk/guidance/phishing* (accessed on Feb 2019).

Oest A, Safaei Y, Doupé A, Ahn G, Wardman B, Warner G. 2018. Inside a phisher's mind: understanding the anti-phishing ecosystem through phishing kit analysis. In: *APWG symposium on electronic crime research, eCrime 2018, May 15–17, 2018*. San Diego, CA, USA: IEEE, 1–12 DOI 10.1109/ecrime.2018.8376206.

Oest A, Safaei Y, Doupé A, Ahn G-J, Wardman B, Tyers K. 2019. PhishFarm: a scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists. In: *IEEE symposium on security and privacy (SP)*. Piscataway: IEEE, 1344–1361 DOI 10.1109/SP.2019.00049.

Ohmori M. 2023. Let's block encrypted malicious sites. In: *2023 IEEE 47th annual computers, software, and applications conference (COMPSAC)*. Piscataway: IEEE, 1878–1883 DOI 10.1109/COMPSAC57700.2023.00293.

Okoli C. 2015. A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems* **37(1)**:879–910 DOI 10.17705/1CAIS.03743.

Onaolapo J, Mariconti E, Stringhini G. 2016. What happens after you are pwnd: understanding the use of leaked webmail credentials in the wild. In: *Proceedings of the 2016 ACM on internet measurement conference, IMC 2016, Santa Monica, CA, USA, November 14–16, 2016*. New York: ACM, 65–79.

Pantic N, Husain M. 2018. A decision support system for personality based phishing susceptibility analysis. In: *IEEE international conference on big data (Big Data)*. Piscataway: IEEE, 3066–3071 DOI 10.1109/BigData.2018.8622555.

Park G, Stuart LM, Taylor JM, Raskin V. 2014. Comparing machine and human ability to detect phishing emails. In: *2014 IEEE international conference on systems, man, and cybernetics, SMC 2014, October 5-8, 2014*. Piscataway: IEEE, 2322–2327 DOI 10.1109/smc.2014.6974273.

Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, Zwaans T. 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security* **66**:40–51 DOI 10.1016/j.cose.2017.01.004.

Parsons K, McCormac A, Pattinson MR, Butavicius MA, Jerram C. 2015. The design of phishing studies: challenges for researchers. *Computers and Security* **52**:194–206 DOI 10.1016/j.cose.2015.02.008.

Petrič G, Roer K. 2022. The impact of formal and informal organizational norms on susceptibility to phishing: combining survey and field experiment data. *Telematics and Informatics* **67**:1–15 DOI 10.1016/j.tele.2021.101766.

Pires C, Borges J. 2023. Detecting targeted phishing websites for brand protection and cyber defence using computer vision. In: *2023 IEEE international workshop on technologies for defense and security (TechDefense)*. Piscataway: IEEE, 1–6 DOI 10.1109/TechDefense59795.2023.10380893.

Pirocca S, Allodi L, Zannone N. 2020. A toolkit for security awareness training against targeted phishing. Berlin, Heidelberg: Springer-Verlag, 137–159 DOI 10.1007/978-3-030-65610-2_9.

Podila LM, Bandreddi JP, Campos JI, Niyaz Q, Yang X, Trekles A, Czerniak C, Javaid AY. 2020. Practice-oriented smartphone security exercises for developing cybersecurity mindset in high school students. In: *IEEE international conference on teaching, assessment, and learning for engineering (TALE)*. Piscataway: IEEE, 303–310 DOI 10.1109/TALE48869.2020.9368440.

Privalov AN, Smirnov VA. 2022. Detection of Fake Educational Sites Using Fuzzy String Match. In: *2022 2nd international conference on technology enhanced learning in higher education (TELE)*. 31–36 DOI 10.1109/TELE55498.2022.9800955.

Privalov AN, Smirnov VA. 2023. Development of a software tool for searching fake educational domain names. In: *2023 3rd international conference on technology enhanced learning in higher education (TELE)*. 270–275. Phishing detection DOI 10.1109/TELE58910.2023.10184377.

ProofPoint. 2023. State of the phish—an in-depth look at user awareness, vulnerability and resilience. Technical report 1. Proofpoint, Inc. *Available at https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2023.pdf* (accessed on Oct 2023).

ProofPoint. 2024. State of the phish—risky actions, real-world threats and user resilience in an age of human-centric cybersecurity. Technical Report 1. *Available at https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf* (accessed on February 2024).

Purkait S. 2012. Phishing counter measures and their effectiveness—literature review. *Information Management & Computer Security* **20(5)**:382–420 DOI 10.1108/09685221211286548.

Qabajeh I, Thabtah FA, Chiclana F. 2018. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review* **29**:44–55 DOI 10.1016/j.cosrev.2018.05.003.

Rader M, Rahman S. 2015. Exploring historical and emerging phishing techniques and mitigating the associated security risks. ArXiv arXiv:1512.00082.

Ramanathan V, Wechsler H. 2013. Phishing detection and impersonated entity discovery using conditional random field and latent dirichlet allocation. *Computers & Security* **34**:123–139 DOI 10.1016/j.cose.2012.12.002.

Rastenis J, Ramanauskaitė S, Janulevičius J, Čenys A. 2019. Credulity to phishing attacks: a real-world study of personnel with higher education. In: *Open conference of electrical, electronic and information sciences (eStream)*. 1–5 DOI 10.1109/eStream.2019.8732169.

Reeves A, Parsons K, Calic D. 2020. Whose risk is it anyway: how do risk perception and organisational commitment affect employee information security awareness? In: *HCI for cybersecurity, privacy and trust: second international conference, HCI-CPT 2020, held as part of the 22nd HCI international conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 232–249 DOI 10.1007/978-3-030-50309-3_16.

Ribeiro L, Guedes IS, Cardoso CS. 2024. Which factors predict susceptibility to phishing? An empirical study. *Computers & Security* **136**:1–12 DOI 10.1016/j.cose.2023.103558.

Rodríguez-Corzo JA, Rojas AE, Mejía-Moncayo C. 2018. Methodological model based on Gophish to face phishing vulnerabilities in SME. In: *ICAI workshops (ICAIW)*. 1–6 DOI 10.1109/ICAIW.2018.8555006.

Rosser H, Mayor M, Stemmler A, Ahuja V, Grover A, Hale M. 2022. Phish finders: crowd-powered RE for anti-phishing training tools. In: *2022 IEEE 30th international requirements engineering conference workshops (REW)*. Piscataway: IEEE, 130–135 DOI 10.1109/REW56159.2022.00031.

Rutherford S, Lin K, Blaine RW. 2022. Predicting phishing vulnerabilities using machine learning. In: *SoutheastCon 2022*. 779–786 DOI 10.1109/SoutheastCon48659.2022.9764045.

Salau A, Dantu R, Upadhyay K. 2021. Data cooperatives for neighborhood watch. In: *IEEE international conference on blockchain and cryptocurrency (ICBC)*. Piscataway: IEEE, 1–9 DOI 10.1109/ICBC51069.2021.9461056.

Salloum S, Gaber T, Vadera S, Shaalan K. 2022. A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access* **10**:65703–65727 DOI 10.1109/ACCESS.2022.3183083.

Sanchez F, Duan Z. 2012. A sender-centric approach to detecting phishing emails. In: *Proceedings of the 2012 international conference on cyber security, CYBERSECURITY '12*. Piscataway: IEEE, 32–39 DOI 10.1109/CyberSecurity.2012.11.

Scott J, Kyobe M. 2021. Trends in cybersecurity management issues related to human behaviour and machine learning. In: *International conference on electrical, computer and energy technologies (ICECET)*. 1–8 DOI 10.1109/ICECET52533.2021.9698626.

SecAware. 2013. ISO/IEC 27002:2013—information technology—security techniques—code of practice for information security controls (second edition). *Available at https://www.iso27001security.com/html/27002.html* (accessed on May 2020).

Shaikh AN, Shabut AM, Hossain MA. 2016. A literature review on phishing crime, prevention review and investigation of gaps. In: *10th international conference on*

software, knowledge, information management & applications, SKIMA 2016. Chengdu, China: IEEE, 9–15 DOI 10.1109/skima.2016.7916190.

Shakela V, Jazri H. 2019. Assessment of spear phishing user experience and awareness: an evaluation framework model of spear phishing exposure level (SPEL) in the namibian financial industry. In: *International conference on advances in big data, computing and data communication systems (icABCD)*. 1–5 DOI 10.1109/ICABCD.2019.8851058.

Shanthi RR, Sasi NK, Gouthaman P. 2023. A new era of cybersecurity: the influence of artificial intelligence. In: *2023 international conference on networking and communications (ICNWC)*. 1–4 DOI 10.1109/ICNWC57852.2023.10127453.

Shin J, Carley LR, Dobson GB, Carley KM. 2023. Modeling and simulation of the human firewall against phishing attacks in small and medium-sized businesses. In: *2023 annual modeling and simulation conference (ANNSIM)*. 369–380.

Shombot ES, Dusserre G, Bestak R, Ahmed NB. 2024. An application for predicting phishing attacks: a case of implementing a support vector machine learning model. *Cyber Security and Applications* **2**:1–12 DOI 10.1016/j.csa.2024.100036.

Siadati H, Palka S, Siegel A, McCoy D. 2017. Measuring the effectiveness of embedded phishing exercises. In: *10th USENIX workshop on cyber security experimentation and test, CSET, August 14, 2017*. Vancouver, BC, Canada: USENIX Association, 8.

Singh C, Meenu . 2020. Phishing website detection based on machine learning: a survey. In: *6th international conference on advanced computing and communication systems (ICACCS)*. 398–404 DOI 10.1109/ICACCS48705.2020.9074400.

Sirawongphatsara P, Prachayagringkai S, Pornpongtechavanich P, Rompun T, Chaowmak K, Phanthuna N, Daengsi T. 2023. Comparative phishing attack simulations: a case study of critical information infrastructure organization using two different contents. In: *2023 10th international conference on electrical engineering, computer science and informatics (EECSI)*. 278–281 DOI 10.1109/EECSI59885.2023.10295679.

Skula I, Bohacik J, Zabovsky M. 2020. Use of different channels for user awareness and education related to fraud and phishing in a banking institution. In: *18th international conference on emerging elearning technologies and applications (ICETA)*. 606–612 DOI 10.1109/ICETA51985.2020.9379220.

Steer J. 2017. Defending against spear-phishing. *Computer Fraud & Security* **2017(8)**:18–20 DOI 10.1016/S1361-3723(17)30074-X.

Stembert N, Padmos A, Bargh MS, Choenni S, Jansen F. 2015. A study of preventing email (Spear) phishing by enabling human intelligence. In: *Proceedings of the 2015 european intelligence and security informatics conference (EISIC), EISIC '15*. Piscataway: IEEE Computer Society, USA, 113–120 DOI 10.1109/EISIC.2015.38.

Stevens R, Votipka D, Dykstra J, Tomlinson F, Quartararo E, Ahern C, Mazurek ML. 2022. How ready is your ready? Assessing the usability of incident response playbook frameworks. In: Barbosa SDJ, Lampe C, Appert C, Shamma DA, Drucker SM, Williamson JR, Yatani K, eds. *CHI '22: CHI conference on human factors in computing systems, New Orleans, LA, USA, 29 April 2022—5 May 2022*. ACM, 589:1–589:18 DOI 10.1145/3491102.3517559.

Swarnalatha KS, Ramchandra KC, Ansari K, Ojha L, Sharma SS. 2021. Real-time threat intelligence-block phising attacks. In: *IEEE international conference on computation system and information technology for sustainable solutions (CSITSS)*. Piscataway: IEEE, 1–6 DOI 10.1109/CSITSS54238.2021.9683237.

T N N, Bakari D, Shukla C. 2021. Business E-mail compromise—techniques and countermeasures. In: *International conference on advance computing and innovative technologies in engineering (ICACITE)*. 217–222 DOI 10.1109/ICACITE51222.2021.9404587.

Taib R, Yu K, Berkovsky S, Wiggins MW, Bayl-Smith P. 2019. Social engineering and organisational dependencies in phishing attacks. In: *Human-Computer Interaction—INTERACT 2019—17th IFIP TC 13 International Conference, Paphos, Cyprus, September 2–6, 2019, Proceedings, Part I, Lecture Notes in Computer Science, vol. 11746*. Springer, 564–584 DOI 10.1007/978-3-030-29381-9_35.

Tamanna , Kamboj S, Singh L, Kaur T. 2024. Automated fraud detection in financial transactions using machine learning: an ensemble perspective. In: *2024 2nd international conference on artificial intelligence and machine learning applications theme: healthcare and Internet of Things (AIMLA)*. 1–6 DOI 10.1109/AIMLA59606.2024.10531422.

Tanimu J, Shiaeles S. 2022. Phishing detection using machine learning algorithm. In: *2022 IEEE international conference on cyber security and resilience (CSR)*. Piscataway: IEEE, 317–322 DOI 10.1109/CSR54599.2022.9850316.

Teerakanok S, Yasuki H, Uehara T. 2020. A practical solution against business email compromise (BEC) attack using invoice checksum. In: *IEEE 20th international conference on software quality, reliability and security companion (QRS-C)*. Piscataway: IEEE, 160–167 DOI 10.1109/QRS-C51114.2020.00036.

Thakur TN, Yoshiura N. 2021. AntiPhiMBS-Auth: a new anti-phishing model to mitigate phishing attacks in mobile banking system at authentication level. In: *Database systems for advanced applications. DASFAA 2021 international workshops: BDQM, GDMA, MLDLDSA, MobiSocial, and MUST, Taipei, Taiwan, April 11–14, 2021, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 365–380 DOI 10.1007/978-3-030-73216-5_25.

Thejaswini S, Indupriya C. 2019. Big data security issues and natural language processing. In: *3rd international conference on trends in electronics and informatics (ICOEI)*. 1307–1312 DOI 10.1109/ICOEI.2019.8862744.

Thurman A. 2020. The ecosystem of phishing: from Minnows to Marlins. ReliaQuest blog. *Available at https://www.reliaquest.com/blog/the-ecosystem-of-phishing/*.

Tsalis N, Virvilis N, Mylonas A, Apostolopoulos TK, Gritzalis D. 2014. Browser blacklists: the Utopia of phishing protection. In: *E-Business and telecommunications—11th international joint conference, ICETE, revised selected papers. communications in computer and information science, vol. 554*. Vienna, Austria: Springer, 278–293 DOI 10.1007/978-3-319-25915-4_15.

Tudosi A-D, Graur A, Balan DG, Potorac AD. 2023. An email classification framework for phishing detection in virtualized network environments. In: *2023 22nd*

RoEduNet conference: networking in education and research (RoEduNet). 1–5 DOI 10.1109/RoEduNet60162.2023.10274915.

Turner CMB, Turner CF. 2019. Analyzing the impact of experiential pedagogy in teaching socio-cybersecurity: cybersecurity across the curriculum. *Journal of Computing Sciences in Colleges* **34(5)**:12–22.

Underhay L, Pretorius A, Ojo S. 2016. Game-based enabled e-learning model for e-Safety education. In: *2016 IST-Africa week conference*. 1–7 DOI 10.1109/ISTAFRICA.2016.7530603.

Van Der Heijden A, Allodi L. 2019. Cognitive triaging of phishing attacks. In: *Proceedings of the 28th USENIX conference on security symposium, SEC'19*. USENIX Association, USA, 1309–1326.

Vargas J, Bahnsen AC, Villegas S, Ingevaldson D. 2016. Knowing your enemies: leveraging data analysis to expose phishing patterns against a major US financial institution. In: *2016 APWG symposium on electronic crime research (eCrime)*. 1–10 DOI 10.1109/ECRIME.2016.7487942.

Varshney G, Iyer P, Atrey P, Misra M. 2021. Evading DoH via live memory forensics for phishing detection and content filtering. In: *International conference on communication systems NETworkS (COMSNETS)*. 1–4 DOI 10.1109/COMSNETS51098.2021.9352935.

Verizon. 2022. DBIR: data breach investigations report. Technical report. Verizon Trademark Services LLC. *Available at https://www.verizon.com/business/resources/T717/reports/2023-data-breach-investigations-report-dbir.pdf* .

Vos J, Erkin Z, Doerr C. 2021. Compare before you buy: privacy-preserving selection of threat intelligence providers. In: *IEEE international workshop on information forensics and security (WIFS)*. Piscataway: IEEE, 1–6 DOI 10.1109/WIFS53200.2021.9648381.

Wang X, Li WW, Leung ACM, Yue WT. 2024. To alert or alleviate? A natural experiment on the effect of anti-phishing laws on corporate IT and security investments. *Decision Support Systems* **179**:1–14 DOI 10.1016/j.dss.2024.114173.

Williams EJ, Hinds J, Joinson AN. 2018. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies* **120**:1–13 DOI 10.1016/j.ijhcs.2018.06.004.

Williams EJ, Morgan PL, Joinson AN. 2017. Press accept to update now: individual differences in susceptibility to malevolent interruptions. *Decision Support Systems* **96**:119–129 DOI 10.1016/j.dss.2017.02.014.

Williams JA, Zafar H, Gupta S. 2024. Fortifying healthcare: an action research approach to developing an effective SETA program. *Computers & Security* **138**:103655 DOI 10.1016/j.cose.2023.103655.

Wu P, Guo H. 2022. HOLMES: an efficient and lightweight semantic based anomalous email detector. In: *2022 IEEE smartworld, ubiquitous intelligence & computing, scalable computing & communications, digital twin, privacy computing, metaverse, autonomous & trusted vehicles*. Piscataway: IEEE, 2293–2300. *Available at https://ieeexplore.ieee.org/document/10189472*.

Xu J, Qi J, Xi Y. 2016. OTP bidirectional authentication scheme based on MAC address. In: *2016 2nd IEEE international conference on computer and communications (ICCC)*. Piscataway: IEEE, 1148–1152 DOI 10.1109/CompComm.2016.7924884.

Yaser Al-Bustani AM, Almutairi AK, Alrashed A, Muzaffar AW. 2023. Social engineering via personality psychology—bypassing users based on their personality pattern to raise security awareness. In: *2023 international conference on IT innovation and knowledge discovery (ITIKD)*. 1–8 DOI 10.1109/ITIKD56332.2023.10100048.

Yu S, Kwon Y, Kim M, Lee K. 2024. Korean voice phishing detection applying NER with key tags and sentence-level N-Gram. *IEEE Access* **12**:52951–52962 DOI 10.1109/ACCESS.2024.3387027.

Zeng YG. 2017. Identifying email threats using predictive analysis. In: *2017 international conference on cyber security and protection of digital services (Cyber Security)*. 1–2 DOI 10.1109/CyberSecPODS.2017.8074848.

Zhang J, Berthier R, Rhee W, Bailey M, Pal P, Jahanian F, Sanders WH. 2012. Safeguarding academic accounts and resources with the university credential abuse auditing system. In: *Proceedings of the 2012 42nd annual IEEE/IFIP international conference on dependable systems and networks (DSN), DSN '12*. Piscataway: IEEE Computer Society, 1–8.

Zhou L, Zhang D, Liu Z. 2023. A stage model for understanding phishing victimization behavior in embedded training. In: *2023 IEEE international conference on intelligence and security informatics (ISI)*. Piscataway: IEEE, 1–6 DOI 10.1109/ISI58743.2023.10297204.

Zhuang W, Ye Y, Chen Y, Li T. 2012. Ensemble clustering for internet security applications. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* **42(6)**:1784–1796 DOI 10.1109/TSMCC.2012.2222025.