IMPROVING PHISHING REPORTING IN HIGHER EDUCATION:

A USER-CENTERED DESIGN APPROACH

By

RACHEL MEI LEE WHITAKER

A Thesis Submitted to The W.A. Franke Honors College

In Partial Fulfillment of the bachelor's degree
With Honors in

Computer Science

THE UNIVERSITY OF ARIZONA

D E C E M B E R 2 0 2 4

Approved by:

Dr. Sazzadur Rahaman
Computer Science Department

1 Abstract

Phishing attacks are a persistent cybersecurity challenge, leveraging human psychology and technological gaps to exploit unsuspecting users. Higher education institutions (HEIs) face unique vulnerabilities due to their decentralized structures, diverse user populations, and dynamic environments. This literature review examines existing phishing reporting technologies in HEIs, highlighting deficiencies in usability, user engagement, and systemic support. Despite advancements in automated detection and awareness training, user interaction with reporting tools remains underexplored, limiting their effectiveness.

Drawing on research and practical experience at the University of Arizona's Security Operations Center (SOC), this work identifies key barriers to phishing reporting, including inconsistent email and OS interfaces, users' psychological deterrents, and limited user knowledge. It emphasizes the importance of user-centered design in reporting mechanisms, proposing that intuitive, accessible tools (such as single-button reporting systems) can significantly enhance user participation and institutional defenses.

The study also evaluates behavioral and demographic factors influencing phishing susceptibility and reporting, noting gaps in targeted awareness initiatives. To address these challenges, a two-phase experiment is proposed, combining surveys and focus groups to analyze user interactions with phishing reporting systems. This approach seeks to uncover actionable insights for improving reporting rates and cybersecurity outcomes.

By bridging the gap between technical solutions and user behaviors, this research contributes to the development of effective phishing mitigation strategies tailored to the needs of HEIs. Its findings have broader implications, offering a framework for enhancing user engagement and institutional resilience in combating phishing across diverse sectors.

2 Introduction

Phishing attacks are a pervasive form of social engineering designed to steal login credentials, deliver malicious software, or extort money from victims. These attacks take various forms, including Smishing (via text messages), phishing (via email), and Vishing (via phone calls). Phishers exploit legitimate services such as Google Forms or DocuSign, impersonate trusted entities, or manipulate victims with threats or urgent requests. Security Operation Center (SOC) teams continually adapt to these evolving threats, but attackers persistently refine their techniques to outsmart defenses.

It is well-documented in cybersecurity that humans are often the weakest link in security—not due to negligence or incompetence, but because of inherent psychological tendencies. Humans are naturally influenced by trust, urgency, and other social cues, which attackers skillfully exploit. Regardless of advances in automation to filter phishing emails or efforts to increase user awareness, people can make mistakes, especially when busy or overwhelmed. Phishing attacks are designed to take advantage of these moments, making even well-trained individuals vulnerable. This is not an indictment of users but a reflection of the evolving sophistication of phishing campaigns and the psychological tactics they employ.

Higher education institutions (HEIs) face unique challenges in combating phishing attacks due to their open, decentralized nature and diverse populations. Universities function like small cities, encompassing independent departments, varied email systems, and a wide range of user behaviors. Students, particularly those new to managing their own accounts, are especially susceptible to scams like fraudulent job offers. Decentralized IT systems within an HEI often mean that individual departments have their own IT teams and unique approaches to handling phishing incidents. As a result, faculty or staff may forward phishing emails to their departmental IT support instead of the central SOC. This fragmentation can delay or even prevent a unified response to phishing threats, as critical information about ongoing attacks may not reach the SOC in time to mitigate the risk effectively across the institution.

HEIs also grapple with a constantly changing population and a bring-your-own-device (BYOD) environment, which complicates the implementation of an effective email management system. University resources can be accessed through a wide range of personal and institutional devices, including laptops, smartphones, tablets, and desktops, each with varying software, operating systems, and configurations. This diversity makes it challenging to deploy a unified email reporting mechanism, as not all devices support standardized features like a"report phishing" button. For example, email management systems tailored for desktop applications may not translate seamlessly to mobile platforms, and users accessing email through third-party apps may lack any integrated reporting functionality. Additionally, ensuring compatibility across multiple email clients and devices while maintaining security protocols, such as encryption and authentication, adds further complexity to deploying a consistent, user-friendly reporting system.

The psychology of phishing reporting further complicates matters. Many users are unaware of phishing reporting tools or processes. Others believe that if they have not fallen victim to a phishing email, there is no need to report it. Fear of embarrassment—such as reporting a legitimate email as phishing by mistake—also discourages some users from taking action. The transient nature of the student population means that education and awareness campaigns must be continually repeated, yet they often fail to reach everyone effectively.

The purpose of this literature review is to examine existing phishing reporting mechanisms, particularly their application in HEIs, and identify gaps in current research. While much work has been done on phishing detection using machine learning, automating responses, and improving user training, few studies have explored the comparative effectiveness of email management tools or the role of user engagement in phishing reporting systems. By understanding user needs and behaviors, this review aims to propose practical improvements to phishing reporting mechanisms that could enhance cybersecurity in HEIs. Drawing on my experience as a student analyst at the University of Arizona's SOC, this thesis bridges the gap between existing technological solutions and their real-world application in higher education settings.

This literature review evaluates the effectiveness of phishing reporting technologies in HEIs, focusing on gaps in user engagement and reporting mechanisms. It argues that understanding user needs and preferences is essential to improving reporting rates and overall cybersecurity. Making phishing reporting intuitive and accessible is as important as automating defenses and raising user awareness, emphasizing the critical human factor in phishing prevention.

3 Literature Review

3.1 Attackers' Perspective and Challenges for Defenders

The digital battlefield between attackers and defenders in the phishing ecosystem is marked by constant adaptation, innovation, and exploitation of systemic weaknesses. Understanding the intricate dynamics at play is crucial for developing more effective defense mechanisms. Below, I explore the attackers' strategies and the hurdles defenders face in countering these threats.

3.1.1 How Attackers Operate

Phishing kits have revolutionized how attacks are conducted by lowering the technical barriers for would-be attackers. As highlighted by Cova et al. (2008), these prepackaged tools mimic the appearance of trusted institutions like banks or social platforms. However, the study also uncovered a sinister twist: many "free" phishing kits come with hidden backdoors, allowing the kit creators to harvest data from other attackers' victims. This creates a secondary exploitation layer, making phishing an even more challenging problem [7].

Han, Kheir, and Balzarotti (2016) expanded on this topic by introducing *PhishEye*, a system designed to ethically monitor phishing kit activity. Their findings revealed how attackers evade detection through techniques like server-side filtering and exploiting delays in blacklists, allowing phishing sites to remain active just long enough to victimize unsuspecting users. The brief operational window of these kits—often peaking at 8–10 days—underscores the attackers' reliance on speed and stealth [10].

3.1.2 Defensive Challenges

On the defensive side, Moore and Clayton (2007a) provide a sobering analysis of the limitations in current strategies. Phishing site takedowns, while effective in the short term, are plagued by delays that give attackers ample time to gather sensitive data. Moreover, advanced techniques such as "Rock Phish" and "Fast Flux" domains allow attackers to constantly shift their infrastructure, making it harder for defenders to keep up. These inefficiencies are compounded by economic factors, with phishing scams costing banks millions annually [20].

Collaboration among defenders is another significant challenge. Moore and Clayton (2007b) stress the importance of cooperation between stakeholders, including banks, ISPs, and domain registrars. However, inconsistent priorities and varying response times hinder the overall effectiveness of these efforts. This lack of coordination leaves gaps that attackers are quick to exploit [19].

3.1.3 Innovations and Countermeasures

While the challenges are immense, there is hope in the form of innovative countermeasures. Huang, Tan, and Liu (2009) categorize defensive strategies

into server-side, browser-side, and user training approaches. Their work emphasizes the potential of technologies like webpage watermarking to provide robust, proactive defenses against deceptive phishing attacks [11]. Meanwhile, Oest et al. (2018) highlight the importance of understanding attackers' behaviors to inform better defensive strategies, including real-time detection and response systems [21].

3.2 Automation and Detection

Phishing, a persistent cybersecurity challenge, exploits human vulnerabilities and technological gaps. To counter this, researchers have developed methods to automate phishing detection, focusing on email filtering and webpage detection. These two areas showcase the diversity and depth of approaches that aim to outpace attackers' evolving strategies. Additionally, there has been a growing focus on using AI and deep learning techniques for phishing detection, particularly with advancements like ChatGPT and other large language models.

3.2.1 Email Filtering

Emails remain the most common vector for phishing attacks. Researchers such as Almomani et al. [1] have extensively reviewed phishing email filtering techniques, emphasizing the critical role of machine learning in distinguishing legitimate communications from malicious ones. Their work categorizes approaches into network-level protection, client-side tools, and server-side classifiers. Notably, they highlight the ongoing challenge of zero-day phishing emails-phishing that exploit previously unknown vulnerabilities —and stress the need for adaptive, real-time solutions.

Similarly, Birthriya and Jain [2] explored advancements in rule-based, machine learning, and deep learning models for email filtering. They argue for a shift from static rule-based systems to dynamic, adaptive methods capable of learning from new attack patterns. Their findings align with others in the field, suggesting that while automation is crucial, resilience against sophisticated attacks is equally important.

Despite these advancements, challenges persist. Many filtering systems face high false positive rates, particularly with emails containing embedded links that mimic legitimate URLs. As Almomani et al. [1] note, the effectiveness of these systems hinges on continuous updates and access to diverse training datasets. This need for constant evolution reflects the relentless nature of phishing threats.

3.2.2 Phishing Webpage Detection

Phishing webpages, which often masquerade as legitimate sites, present distinct detection challenges. Xiang and Hong [27] introduced a hybrid detection approach combining identity discovery and keyword retrieval. Their innovative system bypasses the need for extensive training data, instead leveraging information retrieval algorithms to identify inconsistencies between a webpage's

claimed identity and its actual nature. By focusing on domain name discrepancies and using a Whitelist approach, their method achieves a notable balance of high true positive rates and low false positive rates, suggesting that this system catches a high percentage of phishing domains with a high rate of precision.

Marchal et al. [17] advanced the field with a language- and brand-independent model powered by gradient-boosting machine learning. Their system excels in detecting phishing pages with minimal training data and demonstrates how exploiting phishers' inherent limitations—such as restricted control over URLs—can lead to scalable and efficient detection mechanisms. Their model, with its privacy-friendly and client-side implementation, sets a benchmark for future research.

However, not all tools are without flaws. Studies on anti-phishing toolbars, such as those by Cranor et al. [4], reveal significant usability and accessibility issues. While tools like SpoofGuard achieve high detection accuracy, their high false positive rates and reliance on user interaction hinder their overall effectiveness. These findings underscore the importance of designing tools that balance detection performance with user trust and usability.

3.2.3 Automation and Detection in the Security Framework

The landscape of phishing detection is as dynamic as the phishing emails and scammers it seeks to counter. Across email filtering and webpage detection, a recurring theme emerges: the need for adaptability and user-centric design. While automation offers immense potential, its true value lies in seamlessly integrating these systems into daily workflows without compromising accuracy or accessibility.

Beyond technology, organizational strategies are critical in managing phishing threats. Ohaya [22] emphasizes the importance of fostering a security-aware culture within organizations. Despite advanced detection tools, phishing remains a significant threat due to employees' limited technical knowledge and susceptibility to sophisticated scams. This gap highlights the need for a combined approach: robust technical defenses paired with comprehensive user education programs. As research progresses, the integration of these strategies—automation and awareness—can provide a robust defense against the ever-evolving menace of phishing.

3.3 User Awareness

Phishing exploits human vulnerabilities, and in higher education institutions (HEIs), these vulnerabilities are amplified by the diversity of users and decentralized structures. This section explores the literature surrounding user awareness, structured around four key areas: simulated phishing campaigns, educational institutions, behavioral studies, and sustaining awareness. Emphasis is placed on sustaining awareness, as most research underscores its central role in fostering long-term cybersecurity practices.

3.3.1 Simulated Phishing Campaigns

Simulated phishing campaigns are widely recognized as a practical approach to increasing user vigilance. For example, Dodge et al. [9] observed a marked decrease in user susceptibility to phishing when simulations were conducted regularly. Similarly, Kumaraguru et al. [14, 15] evaluated tools like PhishGuru and Anti-Phishing Phil, which deliver immediate, interactive feedback during teachable moments. While PhishGuru redirected users to instructional materials upon clicking phishing links, Anti-Phishing Phil engaged users through a game that taught phishing recognition. Both tools demonstrated significant improvements in detection capabilities.

Gamification further enhances these efforts. Jensen et al. [13] developed a reporting system with incentives like public recognition and rewards, leading to higher reporting rates and engagement. Although this approach sometimes increases false positives, it underscores the potential of gamified systems to maintain user interest. Other work [12] emphasizes the value of validating user reports to build confidence and accuracy in phishing detection. Despite their benefits, these campaigns face challenges in HEIs, where decentralized structures and resource limitations can hinder implementation.

3.3.2 Educational Institutions

Higher education institutions (HEIs) present a complex landscape for combating phishing due to their diverse user populations, decentralized operational structures, and often limited resources. Studies consistently identify students as a particularly vulnerable group within HEIs. Diaz et al. [8] observed that students' susceptibility to phishing attacks is shaped by factors such as their academic year, department, and exposure to cybersecurity training. Similarly, Broadhurst et al. [5] reported that first-year and international students are especially at risk, largely due to their unfamiliarity with institutional systems. These findings underscore the necessity for targeted awareness campaigns that account for the unique demographic vulnerabilities of these groups while fostering a culture that supports phishing prevention and encourages proactive reporting behaviors.

Phishing mitigation relies heavily on users reporting suspicious emails, but this behavior is underutilized in HEIs. Jensen et al. [13] demonstrated that gamified reporting systems, integrating features like leaderboards and rewards, effectively boost reporting rates. Public acknowledgment and validation of user reports were particularly impactful in encouraging engagement. Similarly, Jensen et al. [12] emphasized the value of centralized knowledge-sharing platforms that validate user reports, promote collaboration, and mitigate uncertainty in reporting. Despite these promising strategies, the decentralized structure and political sensitivities inherent in HEIs complicate the deployment of such solutions. Kwak et al. [16] noted that psychological barriers, including fear of ridicule and wasted effort, further deter users from reporting phishing emails. Simplifying reporting mechanisms and providing acknowledgment for submitted

reports could address these barriers, making reporting more accessible and less intimidating.

The usability of anti-phishing tools remains a significant challenge in HEIs. Chaudhary et al. [6] identified issues such as overcomplicated user interfaces, ambiguous warning messages, and insufficient guidance, which discourage users from interacting with these systems. Simplifying these tools and involving diverse stakeholders during the design process could enhance their effectiveness. However, resource constraints typical of HEIs must also be considered, as implementing advanced tools is often cost-prohibitive. Non-technical barriers to phishing management further complicate these efforts. Pattinson [23] examined cognitive and psychological factors influencing phishing detection and reporting, finding that personality traits such as conscientiousness and extraversion positively impacted user engagement, while institutional culture played a critical role in fostering proactive behaviors. Effective solutions for HEIs must prioritize user-centered approaches, such as streamlined reporting tools and consistent training initiatives.

Behavioral studies provide additional insights into user interactions with phishing emails within HEIs. Marin et al. [18] investigated the roles of self-efficacy, subjective norms, and organizational culture in influencing users' likelihood of reporting phishing emails. Although this research focused on corporate settings, its findings highlight the importance of fostering supportive institutional norms that encourage reporting behaviors. Meanwhile, Blythe et al. [3] discussed the methodological challenges of studying phishing reporting, including underreporting and difficulties in obtaining accurate data. These challenges are particularly relevant in HEIs, where diverse user groups and decentralized systems complicate efforts to monitor and improve reporting.

Systemic vulnerabilities further exacerbate phishing risks in HEIs. Wang et al. [26] critiques the absence of enforceable cybersecurity mandates within U.S. regulations for HEIs, which hampers the implementation of comprehensive training and reporting systems. Students, often the primary targets of phishing attacks, frequently lack access to the same cybersecurity training provided to staff, leaving significant gaps in institutional defenses. Moreover, many institutions rely on cybersecurity insurance as a reactive measure rather than adopting proactive educational initiatives. This reliance underscores the urgent need for robust legal frameworks and institutional reforms to address these systemic weaknesses and ensure HEIs are equipped to combat phishing effectively.

3.3.3 Behavioral Studies

Behavioral studies provide critical insights into how users perceive and respond to phishing attempts. Sheng et al. [25] found that demographics such as age and gender influence phishing susceptibility, with younger users and women being more prone due to lower technical knowledge and Internet experience. Similarly, personality traits like conscientiousness and extraversion have been linked to better phishing Email Management [23]. These findings suggest that targeted training could address specific vulnerabilities.

Reporting behavior is another area of focus. Kwak et al. [16] identified fear of negative outcomes—such as ridicule or wasted effort—as a significant barrier to reporting phishing emails. Simplified reporting mechanisms and features like gamified rewards have shown promise in overcoming these barriers [13]. However, tailoring these approaches to individual traits, as suggested by Marin et al. [18], poses practical challenges in resource-limited environments like HEIs.

3.3.4 Sustaining Awareness

The majority of user awareness literature emphasizes the importance of sustaining awareness. Initial training programs, while effective, often lose impact over time. Reinheimer et al. [24] demonstrated that training effects diminish within six months, highlighting the need for ongoing reinforcement. Interactive and video-based examples have been particularly effective in maintaining user vigilance.

Gamification offers a compelling strategy for long-term engagement. For instance, Anti-Phishing Phil provides an enjoyable learning experience that helps users retain phishing recognition skills over time [15]. Similarly, gamified reporting systems have been shown to sustain participation and improve outcomes [13]. Institutional culture also plays a crucial role. Chaudhary [6] advocates for the integration of usability in security system design, while Wang [26] calls for stronger regulatory frameworks to institutionalize sustained awareness initiatives.

3.4 Gaps and Limitations

3.4.1 HEIs vs Companies in Terms of Phishing and Reporting

While research studies have extensively explored phishing in corporate settings, there is a noticeable gap in addressing the unique challenges faced by higher education institutions (HEIs). Studies such as those by Diaz et al. [8] and Broadhurst et al. [5] highlight the fast-changing student population in HEIs, underscoring the difficulty of maintaining continuity in cybersecurity education. These studies also emphasize the need to educate faculty and staff, who are often overlooked in phishing awareness campaigns.

Conversely, research on corporate environments, such as Jensen et al. [12], demonstrates the relative success of structured reporting systems and their positive impact on user engagement and detection rates. However, the applicability of these systems to HEIs remains underexplored, particularly due to the decentralized nature of universities and the diversity of their user bases.

Furthermore, while corporate studies frequently discuss the technologies used for phishing reporting, there is scant discussion of similar systems tailored for HEIs. This technological gap highlights a critical area for development, as universities often lack the streamlined tools available in corporate settings to encourage and simplify the reporting process.

3.4.2 Holistic Analysis of University Populations

Most studies tend to segment their focus on either student or staff awareness, rarely addressing the entire university population as a cohesive entity. For example, Diaz et al. [8] primarily discuss student susceptibility, while Chaudhary et al. [6] focus on usability challenges faced by staff. This fragmented approach neglects the interconnected nature of university operations, where phishing vulnerabilities in one group can impact the broader institutional ecosystem.

Additionally, much of the current literature prioritizes awareness over reporting mechanisms. While awareness campaigns such as those explored by Kumaraguru et al. [14] effectively reduce susceptibility, they do not address the technological barriers that hinder effective reporting. Studies like Marin et al. [18] delve into the psychological motivations behind reporting but stop short of evaluating the intuitiveness or usability of reporting tools in HEI contexts. This gap highlights the need for user-centered design in reporting systems that cater to the unique demographics of universities.

3.4.3 HEI-Specific Reporting Improvements

The challenges of studying phishing in HEIs are compounded by the difficulties of empirically measuring reporting behaviors in real-world conditions. As Blythe et al. [3] note, many studies rely on artificial scenarios that do not fully capture the complexities of phishing in decentralized institutions. This limitation extends to evaluating the effectiveness of reporting systems, which often suffer from a lack of real-world validation.

Moreover, while corporate-focused studies frequently suggest enhancements to reporting mechanisms, such as gamification and centralized platforms (e.g., Jensen et al. [13]), there is limited research on how these improvements can be adapted for HEIs. For instance, HEIs face unique barriers such as high student turnover, resource constraints, and decentralized IT governance, which complicate the implementation of robust reporting systems. Addressing these institution-specific challenges requires a dedicated research focus on developing intuitive, accessible, and cost-effective reporting tools tailored to the needs of HEIs.

4 Potential Impact

This paper points out a significant gap in the literature: the lack of research on how users interact with phishing reporting technology in higher education institutions (HEIs) from a qualitative, human-centric design perspective. Previous research on reporting technology has predominantly focused on quantitative evaluations of its effectiveness, primarily in corporate environments. Future studies need to explore the reasons users choose to engage—or not engage—with reporting systems. This would bridge the critical connection between users and Security Operations Centers (SOCs), which rely on user reports to defend against phishing attacks.

As the literature overwhelmingly agrees, user awareness is a cornerstone of phishing defense across both corporate and educational settings. Instead of merely analyzing the effectiveness of reporting systems and inferring potential improvements, a differing approach is to directly engage users to understand what design elements would make these systems intuitive and user-friendly. By applying human-centric design principles, the proposed research prioritizes usability for a diverse population, addressing one of the persistent shortcomings in current anti-phishing technology—interfaces that are too complex or unintuitive for end users.

A human-centric approach is particularly critical in HEIs due to the diversity of email and operating systems used across their populations. Unlike corporations, which can mandate specific email platforms (e.g., Outlook, Gmail) that integrate seamlessly with commercial reporting tools, HEIs often lack the ability to standardize such systems. Students, faculty, and staff frequently rely on their own devices and platforms, creating unique challenges for phishing reporting. Developing a system that functions effectively across diverse platforms within HEIs has the potential to not only address these challenges but also inform best practices across industries.

It is necessary to focus on the importance of co-creating solutions with end users to ensure technology serves its intended audience effectively. This paradigm shift from designing tools for developers to designing tools for users can drive meaningful improvements in phishing defenses, foster broader adoption of these systems, and ultimately strengthen institutional resilience against phishing threats.

Glossary

Email Management The process of organizing, handling, and maintaining email communications effectively. Organizations will often use software with build in anti-phishing technology to manage emails and limit spam and phishing. 9

Fast Flux is a technique used by attacker to hide malware delivery and phishing websites by rapidly cycling through IP addresses tied to a malicious domain (Fortinet Definition). 5

HEI A Higher Education Institution (according to Britannica) is a postsecondary institution that provides education leading to degrees, diplomas, or certificates of advanced study. 3

ISP Internet Service Provider, a company that provides services for accessing and using the internet. 5

Phish Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity in digital communication. 3

Rock Phish A type of phishing attack conducted through SMS messages to deceive individuals into sharing sensitive information. 5

Smishing A type of phishing attack conducted through SMS messages to deceive individuals into sharing sensitive information. 3

Vishing A type of phishing attack conducted through voice calls to obtain sensitive information. 3

Whitelist A list of approved or trusted entities, often used in cybersecurity to permit secure access. 7

References

[1] Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., and Alaraj, A. M. (2013). A survey of phishing email filtering techniques. *IEEE Communications Surveys & Tutorials*, 15(4):2070–2090.

[2] Birthriya, S. K. and Jain, A. K. (2022). A comprehensive survey of phishing email detection and protection techniques. *Information Security Journal: A Global Perspective*, 31(4):411–440.

[3] Blythe, J., Petrie, A., and Clark, J. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, 52:194–206.

[4] Blythe, M., Petrie, H., and Clark, J. A. (2011). F for fake: Four studies on how we fall for phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2011)*, pages 3469–3478.

[5] Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., and Ipsen, Y. (2019). Phishing and cybercrime risks in a university student community. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2(1):4–23.

[6] Chaudhary, S. (2016). *The use of usable security and security education to fight phishing attacks.* PhD thesis, University of Tampere, Finland.

[7] Cova, M., Kruegel, C., and Vigna, G. (2008). There is no free phish: An analysis of "free" and live phishing kits. In *Proceedings of the Workshop on Offensive Technologies (WOOT).*

[8] Diaz, A., Sherman, A. T., and Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1):53–67.

[9] Dodge, R. C., J., Carver, C., J., and Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1):73–80.

[10] Han, X., Kheir, N., and Balzarotti, D. (2016). Phisheye: Live monitoring of sandboxed phishing kits. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1402–1412. ACM.

[11] Huang, H., Tan, J., and Liu, L. (2009). Countermeasure techniques for deceptive phishing attack. In *2009 International Conference on New Trends in Information and Service Science*, pages 636–641. IEEE.

[12] Jensen, M. L., Durcikova, A., and Wright, R. T. (2017). Combating phishing attacks: A knowledge management approach. In *Proceedings of the 50th Hawaii International Conference on System Sciences.*

[13] Jensen, M. L., Durcikova, A., Wright, R. T., and Kim, H. (2022). Improving phishing reporting using security gamification. *Journal of Management Information Systems*, 39(3):793–823.

[14] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., and Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 1–14.

[15] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., and Hong, J. (2010). Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2):Article 7.

[16] Kwak, Y., Lee, S., Damiano, A., and Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, 48:101343.

[17] Marchal, S., Francois, J., Wagner, C., and Engel, T. (2016). Know your phish: Novel techniques for detecting phishing sites and their targets. In *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, pages 323–333.

[18] Marin, I., Burda, P., Allodi, L., and Zannone, N. (2023). The influence of human factors on the intention to report phishing emails. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*, pages 1–18.

[19] Moore, T. and Clayton, R. (2007a). An empirical analysis of the current state of phishing attack and defence. In *Proceedings of the 2007 Workshop on Economics of Information Security (WEIS)*.

[20] Moore, T. and Clayton, R. (2007b). Examining the impact of website take-down on phishing. In *APWG eCrime Researchers Summit*, pages 1–13.

[21] Oest, A., Safei, Y., Doupe, A., Ahn, G.-J., Wardman, B., and Warner, G. (2018). Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, pages 1–16. IEEE.

[22] Ohaya, C. (2006). Managing phishing threats in an organization. In *InfoSecCD Conference '06*, pages 159–161. ACM.

[23] Pattinson, M., Jerram, C., Parsons, K., McCormac, A., and Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, 20(1):18–28.

[24] Reinheimer, B., Tersch, J., Probst, F., Foehn, M., and Krueger, R. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. In *Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS)*, pages 259–270.

[25] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., and Downs, J. (2010). Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382.

[26] Wang, M. (2023). The lack of responsibility of higher education institutions in addressing phishing emails and data breaches. *Duke Law & Technology Review*, 23(1):35–54.

[27] Xiang, G. and Hong, J. I. (2009). A hybrid phish detection approach by identity discovery and keywords retrieval. In *Proceedings of the 18th International World Wide Web Conference (WWW 2009)*, pages 571–580. ACM.