International Journal of Emerging Trends in Information Technology (IJEIT)
E-ISSN: XXXX-XXX
Vol. 1, Issue 1, April 2025 | pp. 28–42

Research Paper

The Growing Threat of Phishing Attacks and How to Prevent Them

James Carter[1], Olivia Smith[2]

[1] Department of Computer Science, University of Manchester, Manchester, United Kingdom.
[2] School of Informatics, University of Edinburgh, Edinburgh, United Kingdom.

Received: April 01, 2025 / Accepted: April 14, 2025 / Published: April 24, 2025

Abstract

The proliferation of sophisticated cyber threats has positioned phishing attacks as a persistent and significant danger in the digital landscape. This research article provides a comprehensive analysis of the escalating threat posed by phishing, examining its various forms, the underlying psychological principles that attackers exploit, and the effectiveness of current prevention strategies. Through a systematic review of existing literature, this study synthesizes findings on the prevalence, impact, and evolving techniques of phishing attacks. Furthermore, it explores the technological and non-technological methods employed to combat these threats, including user awareness training and legal frameworks. The implications of these findings for individuals, organizations, and future research directions are discussed, highlighting the ongoing need for adaptive and multi-faceted approaches to mitigate the risks associated with phishing.

Keywords: Phishing attacks, Cyber security, Social engineering, Threat prevention, Email ecurity, Cybercrime

Introduction

The digital age has ushered in an era of unprecedented connectivity and convenience, yet it has also spawned a parallel realm of cyber threats that continue to evolve in sophistication and impact (Verizon, 2023). Among these threats, phishing attacks stand out as a particularly pervasive and damaging form of cybercrime. Characterized by deceptive attempts to acquire sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity, phishing poses a significant risk to individuals and organizations alike (Jakobsson & Myers, 2006). The rapid advancement of technology has

not only facilitated legitimate online interactions but has also provided attackers with increasingly sophisticated tools and techniques to carry out their malicious campaigns (Gupta et al., 2018).

Despite significant advancements in cybersecurity measures, phishing attacks persist as a highly successful method for cybercriminals (APWG, 2023). This continued efficacy underscores the inherent challenges in solely relying on technological defenses, as these attacks often exploit human vulnerabilities through social engineering tactics (Hadnagy, 2018). The consequences of successful phishing attempts can be severe, ranging from substantial financial losses and the compromise of sensitive personal data to significant reputational damage for organizations (IBM, 2023). The diverse forms that phishing attacks can take, including email, SMS (smishing), voice calls (vishing), and social media platforms, further complicate the landscape of this threat, requiring a comprehensive understanding of each vector to develop effective countermeasures (Kumar & Carley, 2019).

This research article aims to address the growing concern surrounding phishing attacks by providing an in-depth analysis of the current threat landscape and the various strategies employed to prevent them. Specifically, this research seeks to: analyze the current state and evolution of phishing threats; identify and categorize the diverse types and techniques utilized in phishing attacks; evaluate the effectiveness of different technological and non-technological prevention methods; explore the psychological principles that attackers leverage to manipulate victims; discuss potential future trends in phishing attacks and the corresponding preventative strategies; and review the relevant legal and regulatory frameworks pertaining to phishing and cybersecurity (Hong, 2012). By addressing these objectives, this article intends to provide a comprehensive resource for academic researchers and cybersecurity professionals seeking a deeper understanding of this critical cybersecurity challenge. The subsequent sections of this paper will delve into the existing body of knowledge on phishing attacks, outline the methodology employed for this review, present the findings, discuss their implications, and finally, conclude with key takeaways and directions for future research.

Table 1. *Comparison of Different Types of Phishing Attacks*

Type of Phishing	**Primary Method of Delivery**	**Target Audience**	**Key Characteristics**	**Examples**	**Potential Impact**	**Common Prevention Strategies**
Spear Phishing	Email, Social Media	Specific Individuals	Highly personalized, references	An email to an employee mentioning a specific project	Financial loss, data breach,	Employee training, verifying requests

			personal information	they are working on, requesting urgent action	reputational damage	through multiple channels
Whaling	Email	High-Profile Individuals (e.g., Executives)	Targets senior management, often involves urgent financial requests	An email to the CEO from a supposed legal representative requesting an immediate wire transfer	Significant financial loss, reputational damage, insider threat	Strict verification protocols for financial transactions, executive-specific training
Smishing	SMS/Text Message	General Public	Uses mobile phone text messages, often with a sense of urgency or offering rewards	A text message claiming a package delivery issue and asking for payment information	Financial loss, identity theft, malware installation	Avoiding clicking on links in unsolicited texts, verifying messages with the sender
Vishing	Phone Call	General Public	Uses phone calls to impersonate legitimate organizations	A phone call from someone claiming to be from the IRS demanding immediate payment	Financial loss, identity theft	Being wary of unsolicited calls asking for personal information, verifying the caller's identity
Pharming	DNS Manipulation	General Public	Redirects users to fraudulent websites even with correct URL	Users trying to access a legitimate banking website are unknowingly directed to a fake login page	Financial loss, data theft	Using reputable DNS providers, ensuring secure network configurations

Note. **Table 1** summarizes different phishing attack types, delivery methods, targets, characteristics, examples, impacts, and common prevention strategies. Effective defenses include training, verification protocols, cautious communication practices, and secure network configurations.

Literature Review

A foundational understanding of the multifaceted nature of phishing requires a thorough examination of existing academic literature. This section will delve into the classifications and typologies of phishing attacks, their prevalence and success rates, the psychological principles exploited by attackers, the technologies developed for prevention and detection, and the critical role of user awareness and training.

Phishing attacks are not a monolithic entity; rather, they encompass a range of techniques tailored to specific targets and objectives. Academic literature has extensively categorized these attacks, providing a crucial framework for understanding their nuances (Jakobsson & Myers, 2006; Gupta et al., 2018). For instance, spear phishing involves highly targeted emails or messages designed to deceive specific individuals, often referencing personal information to enhance credibility (Hong, 2012). In contrast, whaling is a type of spear phishing that specifically targets high-profile individuals within an organization, such as CEOs or senior executives, aiming for high-value information or access (Krombholz et al., 2015). Smishing utilizes SMS or text messages to lure victims into revealing sensitive data or downloading malware, while vishing employs phone calls to achieve similar malicious goals (Symantec, 2019). Another notable type is pharming, which involves manipulating DNS records to redirect users to fraudulent websites even if they type the correct URL (Aburrous et al., 2010). The ongoing evolution of these classifications is evident in the emergence of new techniques that leverage social media platforms, instant messaging services, and even augmented reality, demonstrating the adaptive nature of cybercriminals in response to technological advancements and security measures (Almuhimedi et al., 2014). Examining the trends in the frequency and success of these varied phishing types, as reported in the literature, can reveal shifts in attacker focus and the effectiveness of current defenses against specific methods.

Understanding the scale of the phishing problem necessitates an analysis of its prevalence and success rates. Studies across various sectors and demographics consistently report a high incidence of phishing attacks, highlighting their widespread nature (Verizon, 2023; APWG, 2023). Research further indicates that while awareness of phishing is growing, a significant percentage of individuals still fall victim to these scams (Downs et al., 2007). Factors influencing the success rates of phishing attacks include the sophistication of the attack, the victim's level of technical expertise, and their current emotional state (Parsons et al., 2019). Notably, studies have begun to correlate specific user behaviors, such as a tendency to click on unfamiliar

links or a lack of scrutiny towards email sender addresses, with a higher susceptibility to phishing attempts (Sheng et al., 2010). Similarly, organizational vulnerabilities, such as outdated security software or the absence of multi-factor authentication, have been linked to increased risks of successful phishing breaches (IBM, 2023). Identifying these correlations is crucial for developing targeted interventions aimed at both individual users and organizational security practices.

The effectiveness of phishing attacks is heavily reliant on the exploitation of fundamental psychological principles. Attackers often employ social engineering tactics that manipulate human emotions and cognitive biases to bypass rational decision-making (Hadnagy, 2018; Cialdini, 2007). Principles such as urgency are frequently used to pressure victims into immediate action without critical evaluation, for example, by claiming an account will be suspended if immediate action is not taken (Workman, 2008). Authority is another powerful tool, where attackers impersonate legitimate entities like banks or government agencies to gain trust and compliance (Wright & Marett, 2010). Fear of negative consequences, such as financial loss or data compromise, can also be a potent motivator for victims to divulge sensitive information (Mitnick & Simon, 2002). Furthermore, curiosity can be exploited through enticing messages or links that users are compelled to click on. The effectiveness of these tactics can be influenced by cultural and societal factors, as certain authority figures or institutions may hold different levels of trust across different regions (Parsons et al., 2019). A deeper understanding of these psychological underpinnings is vital for designing more effective user awareness training that can equip individuals to recognize and resist these manipulative techniques.

Technological solutions play a critical role in the defense against phishing attacks. A significant body of research focuses on the development and evaluation of various phishing prevention and detection technologies (Basit et al., 2021). Email filtering systems are a primary line of defense, employing algorithms to identify and block suspicious emails based on various characteristics such as sender reputation, content analysis, and the presence of known malicious links or attachments (Aburrous et al., 2010). Anti-malware software provides another layer of protection by detecting and neutralizing malicious software that may be downloaded through phishing attacks. Multi-factor authentication (MFA) significantly enhances security by requiring users to provide multiple forms of verification, making it much harder for attackers to gain unauthorized access even if they obtain login credentials through phishing (Das et al., 2019). URL analysis and reputation services work by examining the characteristics and historical data of website links to identify potentially malicious sites (Rao & Nayak, 2018). While these technologies offer substantial protection, their effectiveness is constantly being challenged by increasingly sophisticated phishing techniques. Some studies report high success rates for certain technologies in blocking known

phishing attempts, while others highlight the limitations in detecting novel or highly targeted attacks, indicating an ongoing arms race between attackers and defenders (Verizon, 2023).

Recognizing the limitations of purely technological defenses, the literature increasingly emphasizes the importance of user awareness and training in mitigating phishing risks (Canfield et al., 2016). Human error remains a significant factor in successful phishing attacks, making well-designed and regularly conducted training programs essential. Research has explored the effectiveness of various training methods, including simulated phishing attacks, interactive modules, and educational materials (Jampen et al., 2020). Studies evaluating these methods often measure their impact on users' ability to identify and report suspicious emails or messages. While some research indicates a positive correlation between training and reduced susceptibility to phishing, other studies suggest that the effectiveness can vary depending on the training content, frequency, and the overall security culture of the organization (Alsharnouby et al., 2015). Emerging approaches to user awareness training are exploring personalized learning paths, gamification techniques, and the integration of behavioral science principles to create more engaging and impactful educational experiences (Jampen et al., 2020).

Methodology

This research article adopts a systematic literature review approach to synthesize existing knowledge on the growing threat of phishing attacks and their prevention. This method was chosen for its ability to provide a comprehensive and objective overview of the current state of research in this field. The rationale behind this approach is to consolidate findings from various studies, identify key trends and patterns, and highlight areas where further investigation is needed.

The identification of relevant literature was conducted through a targeted search across several prominent academic databases and search engines, including Google Scholar, IEEE Xplore, ACM Digital Library, and Web of Science. Additionally, reputable cybersecurity websites such as the SANS Institute and Krebs on Security were consulted to gather insights from industry reports and expert analyses. The primary keywords and search terms used in this process included "phishing attacks," "phishing prevention methods," "social engineering in cybersecurity," "email security best practices," "phishing detection technologies," and "user awareness training for phishing."

The selection of research articles and reports for inclusion in this review was based on specific criteria. The primary focus was on publications within the last five years to ensure the analysis reflects the most current understanding of the phishing landscape. Peer-reviewed articles from academic journals and reputable conference proceedings were prioritized to ensure the quality and rigor of the included research.

Additionally, reports from recognized cybersecurity organizations and government agencies were considered for their practical insights and statistical data. The relevance of each identified source to the research objectives was carefully assessed to ensure that it contributed meaningfully to the analysis of phishing threats and prevention strategies.

The synthesis of the information gathered from the selected literature involved a thematic analysis approach. This method allowed for the identification of recurring themes, key findings, and common perspectives across different sources. The extracted data was analyzed to identify major trends in phishing attack techniques, the reported effectiveness of various prevention methods, the psychological principles most commonly exploited by attackers, and the evolving legal and regulatory landscape. Any contradictions or inconsistencies in the findings across different studies were also noted and considered in the overall analysis. This systematic approach to data synthesis and analysis ensures a comprehensive and well-supported overview of the current state of knowledge regarding phishing attacks and their prevention.

Results

The analysis of the reviewed literature reveals several key findings regarding the current landscape of phishing threats, the effectiveness of prevention methods, the psychological factors contributing to their success, and the relevant legal frameworks.

The current landscape of phishing threats is characterized by increasing sophistication and diversification. While traditional email phishing remains prevalent, there is a marked rise in targeted attacks such as spear phishing and whaling, which often exhibit a high degree of personalization, making them more difficult to detect. Furthermore, phishing attacks are increasingly leveraging multiple channels, including SMS, social media, and even voice calls, indicating a shift towards a more multi-faceted approach by attackers. Reports consistently highlight the significant financial and reputational damage caused by successful phishing incidents across various industries, underscoring the persistent threat these attacks pose. The trend suggests that attackers are continuously adapting their techniques to bypass technological defenses and exploit human vulnerabilities.

The effectiveness of various phishing prevention methods is a subject of ongoing research. Technological solutions such as email filtering and anti-malware software provide a crucial first line of defense, effectively blocking a significant volume of known phishing attempts. Multi-factor authentication has also proven to be highly effective in preventing unauthorized access even when credentials have been compromised through phishing. However, the literature also indicates that these technologies are not foolproof and can be circumvented by sophisticated and novel phishing attacks. User awareness training emerges as a critical

complementary approach, with studies showing that well-designed and regularly conducted training can significantly improve users' ability to recognize and report phishing attempts. There is evidence suggesting that a layered security approach, combining robust technological controls with comprehensive user education, is the most effective strategy for mitigating phishing risks.

Psychological factors play a pivotal role in the success of phishing attacks. Attackers expertly exploit cognitive biases and emotional triggers to manipulate victims into taking actions they would otherwise avoid. Urgency, authority, and fear are consistently identified as key psychological principles leveraged in phishing campaigns. For example, attackers often craft emails or messages that create a sense of urgency, prompting users to act quickly without thinking critically. Impersonating authority figures or trusted organizations is another common tactic used to build credibility and elicit compliance. Understanding these psychological vulnerabilities is crucial for developing more effective user awareness training that specifically addresses these manipulative techniques. Insights from behavioral economics and psychology can be further applied to design more nuanced and impactful anti-phishing interventions.

The legal and regulatory landscape surrounding phishing and cybersecurity is evolving in response to the increasing prevalence and impact of these attacks. Various countries and regions have enacted laws and regulations aimed at criminalizing phishing activities and holding organizations accountable for protecting sensitive data. These frameworks often include provisions for data breach notification, cybersecurity standards, and penalties for cybercrimes. The implications of these legal and regulatory frameworks are significant for both individuals and organizations, setting expectations for data security practices and providing avenues for legal recourse in the event of a phishing attack. Recent developments in this area include stricter enforcement of existing laws and the introduction of new legislation to address emerging cyber threats, reflecting a growing recognition of the need for a strong legal response to combat phishing.

Case studies of successful phishing attacks provide valuable insights into the vulnerabilities that are often exploited and the consequences that can arise. Analysis of these cases reveals recurring themes, such as the exploitation of unpatched software, the lack of multi-factor authentication, and the failure of employees to recognize sophisticated social engineering tactics. Common mistakes that lead to successful breaches include clicking on suspicious links, providing sensitive information in response to unsolicited requests, and failing to verify the legitimacy of communications through alternative channels. These real-world examples underscore the importance of implementing comprehensive security measures and fostering a strong security-conscious culture within organizations.

Table 2. *Effectiveness of Various Phishing Prevention Methods*

Prevention Method	**Reported Effectiveness**	**Advantages**	**Limitations**
Email Filtering	High for known threats	Automatically blocks a large volume of phishing emails	Can be bypassed by sophisticated or novel attacks
Anti-Malware Software	Moderate to High	Detects and removes malicious software downloaded through phishing	May not detect all new or targeted malware
Multi-Factor Authentication (MFA)	Very High	Significantly reduces the risk of unauthorized access even with compromised credentials	Requires user adoption and can sometimes be perceived as inconvenient
User Awareness Training	Moderate to High (with consistent reinforcement)	Educates users to recognize and report phishing attempts	Effectiveness depends on the quality and frequency of training
Phishing Simulation	Moderate to High	Provides practical experience in identifying phishing attempts and tests user vigilance	Needs to be implemented ethically and without shaming employees

Note. Table 2 presents the effectiveness, advantages, and limitations of various phishing prevention methods, highlighting the importance of technical tools and user training.

Table 3. *Psychological Principles Exploited in Phishing Attacks*

Psychological Principle	**Description of the Principle**	**How it is Exploited in Phishing**	**Examples from the Literature**
Urgency	Creating a sense of immediate need for action	Attackers claim immediate action is required to avoid negative consequences (e.g., account closure)	Emails stating "Your account will be suspended if you don't update your information within 24 hours"
Authority	Leveraging the perception of legitimate power or status	Attackers impersonate trusted organizations or figures (e.g., banks, CEOs, government agencies)	Emails appearing to be from a bank requesting verification of account details

Fear	Evoking anxiety or apprehension about potential negative outcomes	Attackers threaten data loss, financial penalties, or other negative repercussions	Emails claiming that a user's computer has been infected with a virus and demanding payment for its removal
Curiosity	Tapping into the natural human desire to learn or investigate	Attackers use enticing subject lines or links that pique users' interest	Emails with subject lines like "See who's been looking at your profile" or links to shocking news stories

Note. Table 3 outlines psychological principles exploited in phishing attacks, such as urgency, authority, fear, and curiosity, which attackers use to manipulate targets.

Discussion

The findings from the literature review highlight the persistent and evolving nature of phishing attacks, underscoring their significant impact on individuals and organizations. The increasing sophistication of these attacks, coupled with their multi-channel delivery, presents a continuous challenge to cybersecurity defenses. While technological solutions offer a crucial layer of protection, their limitations in addressing the human element of phishing are evident. The success of these attacks often hinges on the exploitation of psychological vulnerabilities, emphasizing the critical role of social engineering tactics in their execution.

The analysis of various prevention methods reveals that a multi-layered approach is the most effective strategy. Relying solely on technology is insufficient, as attackers continuously develop new ways to circumvent these defenses. Integrating robust technological controls with comprehensive and ongoing user awareness training is essential to create a more resilient security posture. The effectiveness of user training, however, depends on its quality, relevance, and frequency, suggesting a need for innovative and engaging training methodologies that incorporate insights from behavioral science.

The legal and regulatory frameworks surrounding phishing demonstrate a growing global awareness of the severity of this cybercrime. These frameworks play a vital role in establishing legal boundaries, deterring malicious activities, and providing avenues for recourse. However, the constantly evolving nature of cyber threats necessitates continuous adaptation and strengthening of these legal and regulatory measures to effectively combat phishing and hold perpetrators accountable.

The insights gleaned from case studies of successful phishing attacks provide valuable lessons for both individuals and organizations. Common vulnerabilities and human errors identified in these cases highlight the importance of implementing fundamental security best practices, such as enabling multi-factor

authentication, regularly patching software, and fostering a culture of security awareness. Recognizing the recurring patterns in successful attacks can inform the development of more targeted and effective prevention strategies.

The persistent challenge posed by phishing underscores the need for a dynamic and adaptive approach to cybersecurity. As attackers continue to refine their techniques and exploit new vulnerabilities, defenses must evolve in tandem. Future research should focus on developing more sophisticated detection technologies, enhancing user awareness training through innovative methods, and further strengthening the legal and regulatory frameworks to address this ongoing threat effectively.

Conclusion

This research article has provided a comprehensive analysis of the growing threat of phishing attacks and the various strategies employed to prevent them. The findings underscore the persistent and evolving nature of this cybercrime, highlighting its significant impact on individuals and organizations. While technological solutions play a crucial role in defense, the exploitation of human psychological vulnerabilities remains a key factor in the success of phishing attacks. Therefore, a multi-layered approach that combines robust technological controls with comprehensive user awareness training is essential for effective mitigation. The legal and regulatory landscape is also evolving to address this threat, but continuous adaptation is necessary to keep pace with the ingenuity of cybercriminals. Ultimately, combating phishing requires a holistic approach that recognizes the interplay between technology, human behavior, and legal frameworks, fostering a more secure digital environment for all.

Future Research

Future research should explore the development of more advanced artificial intelligence and machine learning-based detection systems that can identify novel and sophisticated phishing attacks in real-time. Investigating the effectiveness of different user awareness training methodologies, including personalized and gamified approaches, would also be valuable. Further research into the psychological factors that make individuals susceptible to specific types of phishing attacks could inform the development of more targeted interventions. Additionally, exploring the efficacy of international collaborations and harmonized legal frameworks in combating cross-border phishing activities represents an important area for future investigation. Understanding the evolving tactics of phishing attacks in emerging technologies, such as virtual and augmented reality environments, will also be crucial for proactive defense strategies.

Acknowledgment

The author would like to acknowledge the contributions of various researchers and cybersecurity experts whose work has informed this analysis.

Disclosure of Interest

The author declares no conflict of interest.

Funding Information

No funding was received for the preparation of this research article.

References

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. Expert Systems with Applications, 37(12), 7913-7921.

Almuhimedi, H., Liu, B., Sadeh, N., & Hong, J. (2014). Your reputation precedes you: History, reputation, and the dynamics of online transactions. Proceedings of the International Conference on World Wide Web (WWW).

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, 69-82.

Anti-Phishing Working Group (APWG). (2023). Phishing Activity Trends Report. Retrieved from https://apwg.org/trendsreports/

Basit, A., Zafar, M. H., Liu, X., Javed, A. R., & Jalil, Z. (2021). Phishing attack detection: A recent comprehensive study. Journal of Network and Computer Applications, 174, 102887.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. Human Factors, 58(8), 1158-1172.

Cialdini, R. B. (2007). Influence: The Psychology of Persuasion (Rev. ed.). Harper Business.

Das, S., Kim, H., Dabbish, L. A., & Hong, J. I. (2019). The Effect of Social Influence on Security Sensitivity. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW).

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2007). Behavioral response to phishing risk. Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit.

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommunication Systems, 67(2), 247-267. https://doi.org/10.1007/s11235-017-0334-z

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74-81. https://doi.org/10.1145/2063176.2063197

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74-81.

IBM. (2023). Cost of a Data Breach Report 2023. Retrieved from https://www.ibm.com/reports/data-breach

Jakobsson, M., & Myers, S. (Eds.). (2006). Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley.

Jampen, D., Gürgens, S., & Williams, J. (2020). Strengthening End Users Against Phishing Attacks: A Literature Review. Computers & Security, 97, 101923.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Social Engineering Attacks. Journal of Information Security and Applications, 22, 113-122.

Kumar, S., & Carley, K. M. (2019). Social Media–Based Phishing Attacks. Advances in Computers, 112, 1-36. https://doi.org/10.1016/bs.adcom.2018.10.002

Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2019). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 86, 120-127.

Rao, R. S., & Nayak, R. (2018). Multi-level classification model for phishing email detection. Expert Systems with Applications, 91, 153-166.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Symantec. (2019). Internet Security Threat Report. Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence

Verizon. (2023). 2023 Data Breach Investigations Report (DBIR). Retrieved from https://www.verizon.com/business/resources/reports/dbir/

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems, 27(1), 273-303.

Appendix

(No appendix included in this research paper)

Open Access Statement