The Evolution of Phishing and Future Directions: A Review

Jude Osamor[1], Moses Ashawa[1], Alireza Shahrabi[1], Anand Phillip[1] and Celestine Iwend[1,2]
[1]Department of Cybersecurity and Networks, Glasgow Caledonian University, UK
[2]School of Creative Technologies, University of Bolton, UK

jude.osamor@ieee.org (Corresponding author)

Abstract: Phishing has emerged as one of the most persistent and evolving threats in cybersecurity. Its development from simple email scams to highly sophisticated and targeted attacks has been driven by technological advancements, the rise of social media, and the increasing availability of personal data online. This paper provides a comprehensive review of the evolution of phishing, examining key milestones in its history, current trends, and future directions. Emphasis is placed on the integration of emerging technologies such as artificial intelligence (AI) and machine learning (ML), the role of phishing-as-a-service (PhaaS) platforms, and the challenges posed by deepfake phishing and the Internet of Things (IoT). The paper concludes by discussing potential strategies for combating these evolving threats and proposes future research directions to enhance phishing detection and prevention mechanisms. Additionally, the study examines the growing intersection between phishing attacks and state-sponsored cyber operations, highlighting the increasing sophistication of threat actors and their exploitation of geopolitical events for targeted campaigns. The research also addresses the critical need for adaptive defense mechanisms that can respond to the rapid evolution of attack vectors while maintaining usability for legitimate users.

Keywords: Phishing, Spear phishing, Smishing, Whaling, Cybersecurity

1. Introduction

1.1 Background

Phishing represents a significant cybersecurity threat that has evolved considerably from its origins as simple email-based scams (Jakobsson & Myers 2007). The explosive growth of the internet and increasing reliance on digital communication have provided fertile ground for phishing to thrive. According to Hong (2012), phishing attacks have reached unprecedented levels, with the Anti-Phishing Working Group reporting record numbers of unique phishing sites. The widespread use of social media has further complicated the phishing landscape. Social media platforms have become valuable tools for phishers, allowing them to gather detailed information about potential victims and craft highly personalized attacks (Moore & Clayton 2007). The ease with which personal information can be accessed online has made it easier for attackers to exploit human vulnerabilities.

The financial impact of phishing attacks has grown exponentially, with organizations suffering both direct monetary losses and significant damage to their reputation and customer trust. The sophistication of modern phishing techniques has transformed what was once a crude form of cybercrime into a refined art of deception. Attackers now employ advanced social engineering tactics, leveraging psychological principles to manipulate victims into divulging sensitive information or taking harmful actions. The global shift toward remote work and digital services, particularly in recent years, has expanded the attack surface for phishing attempts. Organizations face increasing challenges in protecting their workforce from sophisticated phishing campaigns that target both corporate and personal communication channels. The rise of cloud services and mobile computing has created new vectors for phishing attacks, as users access sensitive information across multiple devices and platforms.

Furthermore, the commercialization of phishing through "Phishing-as-a-Service" platforms has lowered the barrier to entry for cybercriminals, leading to a proliferation of attacks across all sectors of society. This democratization of cybercrime tools has created a complex threat landscape where both sophisticated state actors and amateur criminals can launch effective phishing campaigns.

1.2 Scope and Objectives

This paper aims to provide a comprehensive analysis of phishing evolution and current trends, with specific objectives including an in-depth examination of historical developments, emerging threats, and future countermeasures. The research focuses on understanding how phishing attacks have evolved from simple email deceptions to sophisticated multi-vector threats employing artificial intelligence and social engineering techniques. The primary objectives encompass analyzing the historical development of phishing attacks from their inception to present day, with particular attention to technological and methodological advances. Through examining current trends and emerging threats, the study seeks to identify patterns in attack evolution and predict future developments. The research evaluates the significant impact of new technologies, including artificial intelligence, blockchain, and deepfake capabilities, on both attack methodologies and defense

mechanisms. Finally, this work aims to propose actionable directions for improving phishing prevention and detection strategies across organizational and technical domains.

1.3 Methodology

This research employs a comprehensive literature review methodology, analyzing academic papers, industry reports, and case studies related to phishing. The analysis synthesizes information from multiple authoritative sources to provide a holistic understanding of the phishing threat landscape and its evolution. The methodology incorporates a systematic review of peer-reviewed academic publications from leading cybersecurity journals and conferences, providing theoretical frameworks and empirical evidence for phishing attack patterns and effectiveness. Industry security reports from major cybersecurity firms offer real-world insights into current threats and emerging attack vectors. Data from the Anti-Phishing Working Group provides quantitative metrics on phishing trends and their global impact across different sectors and regions.

The research examines detailed case studies of significant phishing incidents, analyzing attack methodologies, impact assessment, and lessons learned. Technical documentation and standards from relevant organizations are reviewed to understand current best practices and security protocols. This multi-faceted approach ensures a comprehensive understanding of both theoretical foundations and practical implications in the field of phishing security.The analysis emphasizes temporal trends and technological developments, particularly focusing on the intersection of traditional phishing techniques with emerging technologies. Special attention is given to validating findings through cross-referencing multiple sources and identifying consensus among security researchers and practitioners.

2. The Evolution of Phishing

2.1 Early Phishing Attacks (1995-2005)

The first decade of phishing was characterized by relatively simple techniques. Early attacks primarily relied on email as the main vector, with attackers sending large volumes of generic messages hoping to deceive a small percentage of recipients (Rivest 2010). During this foundational period, phishing emerged as a novel threat that would later evolve into a sophisticated cybersecurity challenge. These initial attacks often impersonated AOL administrators, targeting the growing base of internet users who were just beginning to embrace online services and e-commerce. The infamous "Nigerian Prince" scams emerged during this era, establishing many of the social engineering tactics that would become hallmarks of phishing campaigns. Attackers typically used basic HTML formatting and readily identifiable spoofed email addresses, making these early attempts relatively easy to detect for experienced users. The limited sophistication of these attacks was partly due to the nascent state of email authentication protocols and the lack of standardized security measures across email providers. As organizations began implementing basic spam filters and security awareness training, attackers responded by refining their techniques and exploring new vectors for delivering their malicious content.

2.1.1 Basic email spoofing

Early phishers utilized basic email spoofing techniques to impersonate legitimate organizations. These attacks often contained obvious spelling errors and poor formatting, making them relatively easy to identify for attentive users (Emigh 2005). Attackers typically mimicked well-known brands and financial institutions, sending crude imitations of official communications that relied more on volume than sophistication to succeed. The technical barriers to entry were relatively low, with attackers using basic HTML editors and freely available email services to craft their deceptive messages. Spoofed sender addresses were often obvious modifications of legitimate domains, such as "support@arnaz0n.com" or "paypa1-security.com," reflecting the limited understanding of domain registration and email authentication protocols at the time. The landing pages used in these early attacks were typically hosted on free web hosting services and contained copied logos and branding elements of questionable quality. Most attacks focused on harvesting credit card information and login credentials, with little attempt to customize the approach based on the target demographic. The lack of sophisticated tracking mechanisms meant attackers had limited ability to measure campaign effectiveness or adapt their techniques based on success rates. By modern standards, these early spoofing attempts were primitive, but they established the foundational patterns that would evolve into today's more sophisticated phishing campaigns.

2.1.2 Generic mass mailings

Attackers employed mass mailing techniques, sending identical messages to thousands of recipients. The success rate was low but sufficient to make the attacks profitable due to the large volume of attempts (Jakobsson

& Myers 2007). These early campaigns laid the groundwork for more targeted approaches, as attackers learned which tactics generated the highest response rates. The rise of automated mailing tools and readily available email lists from underground markets significantly reduced the operational costs of these mass campaigns. Attackers frequently rotated through different narratives, testing various emotional triggers like urgency, fear, and greed to determine which themes yielded the best results. The emergence of botnets during this period enabled attackers to distribute their mailings across multiple IP addresses, making it more difficult for basic spam filters to block these campaigns effectively. Response rates typically hovered around 0.1%, but with millions of emails sent daily, even this small percentage translated into thousands of potential victims. Phishers began developing rudimentary tracking systems to monitor which email subjects and message templates performed best, leading to the early development of A/B testing in phishing campaigns. The low cost of mass mailing operations meant that even when spam filters became more prevalent, attackers could simply increase their volume to maintain profitable returns.

2.2 Evolution of Sophisticated Techniques (2005-2015)

The second decade saw significant advancement in phishing techniques, driven by improved technology and growing internet adoption. This period marked a crucial transition from simple mass-mailing campaigns to more refined and targeted approaches, fundamentally changing the threat landscape. The emergence of social media platforms provided attackers with rich sources of personal information, enabling them to craft more convincing and contextually relevant phishing attempts. Attackers began leveraging advanced web technologies like JavaScript and CSS to create highly convincing replicas of legitimate websites, making visual detection increasingly difficult for average users. The rise of mobile devices introduced new attack vectors, as smaller screens and limited security interfaces made it harder for users to identify fraudulent content. Sophisticated phishing kits became readily available on underground markets, lowering the technical barrier to entry while simultaneously increasing the quality of attacks. Cloud computing services were increasingly exploited to host phishing infrastructure, providing attackers with reliable, anonymous platforms that could be quickly provisioned and abandoned. The introduction of HTTPS certificates for phishing sites added an additional layer of legitimacy to fraudulent pages, as users had been trained to trust the padlock icon as a signal of security. Criminal organizations began developing specialized roles within their operations, with different teams handling email distribution, website creation, and credential harvesting, leading to more professional and efficient attack campaigns

2.2.1 Spear phishing

This period saw the rise of targeted attacks, known as spear phishing, which focused on specific individuals or organizations. According to Ramzan and Atkinson (2012), these attacks demonstrated significantly higher success rates compared to generic phishing attempts. Attackers began researching their targets extensively, incorporating personal details and organizational context to create more convincing deceptions. The growing availability of professional and personal information on LinkedIn, Facebook, and other social networks provided attackers with unprecedented insight into their targets' roles, relationships, and activities. Cybercriminals started exploiting specific events like mergers, acquisitions, and leadership changes to craft timely and contextually relevant attacks that appeared highly credible to recipients. Advanced persistent threat (APT) groups emerged during this period, using spear phishing as their primary initial access vector to compromise high-value targets in government and industry. Success rates for spear phishing campaigns often exceeded 50% compared to less than 1% for traditional mass phishing, justifying the increased time and resource investment required for target research. The development of automated tools for gathering and analyzing target information from public sources made spear phishing increasingly efficient and scalable. Organizations found traditional security awareness training inadequate against these highly personalized attacks, as legitimate and malicious communications became nearly indistinguishable.

2.2.2 Social engineering tactics

Attackers began incorporating sophisticated social engineering techniques, leveraging psychological manipulation to increase success rates. This included creating a sense of urgency, exploiting authority figures, and using fear tactics (Abu-Nimeh et al. 2007). These psychological approaches proved particularly effective when combined with detailed target research, leading to more successful compromises of both individuals and organizations. Attackers refined their understanding of organizational hierarchies, frequently impersonating executives to pressure employees into taking immediate action without following standard security protocols. The exploitation of business cycles and deadlines became commonplace, with attacks timed to coincide with tax seasons, quarterly financial reporting, or major corporate events when employees were more likely to be

stressed and rushed. Social engineering tactics expanded to include relationship manipulation, where attackers would build rapport over time through multiple interactions before attempting their ultimate deception. Advanced campaigns began incorporating multi-channel approaches, using phone calls (vishing) to reinforce email phishing attempts, creating a more convincing illusion of legitimacy. Cybercriminals developed sophisticated pretext scenarios based on current events and industry trends, making their schemes appear more plausible within the target's professional context. The rise of social media enabled attackers to understand and exploit personal relationships, leading to highly effective impersonation of colleagues, friends, and family members.

2.3 Modern Phishing Landscape (2015-Present)

The current era of phishing is characterized by highly sophisticated attacks that leverage advanced technologies and social engineering techniques. Modern phishing has evolved into a complex threat that combines psychological manipulation with cutting-edge technology, making detection and prevention increasingly challenging. Attackers now employ advanced automation, artificial intelligence, and deep learning to create highly personalized and convincing campaigns that can adapt in real-time to target responses. The emergence of Phishing-as-a-Service (PhaaS) platforms has democratized access to sophisticated attack tools, enabling even novice criminals to launch professional-grade campaigns. Business Email Compromise (BEC) attacks have become increasingly prevalent, with criminals using advanced social engineering and deep fake technology to impersonate executives and authorize fraudulent transactions. The integration of machine learning algorithms allows attackers to automatically generate contextually relevant content and adapt attack strategies based on target responses and behavior patterns. The proliferation of cloud services and collaboration tools, accelerated by the shift to remote work, has created new attack vectors and opportunities for credential harvesting. Ransomware groups have increasingly used sophisticated phishing techniques as their initial attack vector, combining social engineering with advanced malware delivery mechanisms. Mobile-specific phishing attacks have evolved to exploit the unique characteristics of smartphone interfaces and user behaviours, including SMS phishing (smishing) and messaging app-based attacks. The rise of cryptocurrency has introduced new phishing schemes targeting digital wallet credentials and cryptocurrency transactions, with attackers exploiting the irreversible nature of blockchain transactions.

3. Current Trends and Emerging Threats

3.1 AI-Driven Phishing

Modern phishing attacks increasingly leverage artificial intelligence and machine learning capabilities. According to Kotzias et al. (2019), AI-powered systems have transformed the sophistication and scale of phishing campaigns. These systems can now automatically generate highly convincing phishing content by analyzing vast amounts of legitimate communications and mimicking their style and structure. They study target behavior patterns to identify the most vulnerable times and methods for attacks, while continuously adapting their strategies based on success rates. Most concerning is their ability to evade traditional detection methods by learning from and responding to security measures in real-time. Natural Language Processing (NLP) models are being employed to craft messages that match the writing style and tone of impersonated senders, making content-based detection increasingly difficult. Advanced AI systems can now automatically identify and exploit relationships within organizational hierarchies, creating targeted attacks that leverage real business contexts and workflows. The integration of deep learning algorithms enables real-time adaptation of phishing websites, dynamically adjusting their appearance and content based on the visitor's browser fingerprint and behaviour patterns. Machine learning models are being used to automate the process of gathering and analysing target information from multiple sources, creating detailed profiles for more effective social engineering. These AI systems can now predict the most effective attack vectors and timing for specific targets based on historical success rates and behavioural analysis, significantly improving campaign effectiveness.

3.2 Deepfake Phishing

The emergence of deepfake technology has introduced new vectors for phishing attacks. Westerlund (2019) discusses how deepfakes can be used to create highly convincing audio and video content for impersonation attacks. Attackers can now synthesize voice messages that sound identical to company executives or create video clips showing trusted figures making fraudulent requests. This technology makes it increasingly difficult for employees to verify the authenticity of urgent requests or important communications, particularly in organizations with remote work cultures. The development of real-time voice cloning has enabled sophisticated vishing attacks where criminals can engage in live phone conversations while impersonating known individuals.

Video conferencing platforms have become particularly vulnerable to deepfake attacks, as remote workers increasingly rely on virtual meetings for critical business decisions. The combination of deepfake technology with social engineering has led to hybrid attacks where artificial video or audio content is used to validate fraudulent email requests. Advanced GANs (Generative Adversarial Networks) now enable attackers to create and modify facial expressions and gestures in real-time, making video-based verification protocols increasingly unreliable. The proliferation of publicly available voice samples and video footage on social media has provided attackers with ample training data to create increasingly convincing deepfake content targeting specific individuals.

3.3 Mobile Phishing and Smishing

The proliferation of mobile devices has led to new forms of phishing attacks. Marchal et al. (2014) describe how mobile phishing exploits the limitations of mobile interfaces and users' tendency to pay less attention to security indicators on mobile devices. Small screens make it harder to verify website authenticity, while the immediate nature of mobile communications often leads to hasty decisions. SMS-based phishing (smishing) has become particularly effective as users tend to trust text messages more than emails and have fewer tools available to verify message authenticity. The rise of mobile payment systems and digital wallets has created new opportunities for attackers to target financial credentials through specially crafted mobile interfaces. Mobile app-based phishing has emerged as a significant threat, with attackers creating convincing fake applications that mimic legitimate banking, social media, and productivity apps. The integration of QR codes into daily activities has introduced new attack vectors, as users cannot easily distinguish between legitimate and malicious QR codes without scanning them. Push notification phishing has become increasingly sophisticated, exploiting users' habitual responses to mobile alerts and notifications. Mobile browsers' simplified security interfaces often omit crucial security indicators, making it more difficult for users to identify fraudulent websites. The convergence of personal and professional activities on mobile devices has expanded the attack surface, allowing criminals to leverage personal information for workplace-targeted attacks.

3.4 IoT-Based Phishing

The Internet of Things (IoT) has introduced new vulnerabilities that can be exploited for phishing purposes. Hasbini (2021) identifies several key concerns in IoT security that make devices susceptible to phishing attacks. Compromised IoT devices can serve as entry points into larger networks, while their often-limited security features and infrequent updates make them attractive targets. The interconnected nature of IoT systems means that a successful phishing attack on one device can potentially compromise entire networks of connected devices and systems.

4. Prevention and Mitigation Strategies

4.1 Technical Countermeasures

Modern anti-phishing strategies rely on sophisticated technical solutions that work together to create multiple layers of defense. These countermeasures combine traditional security protocols with emerging technologies to provide comprehensive protection against evolving threats. Advanced email authentication frameworks like DMARC (Domain-based Message Authentication, Reporting, and Conformance) provide robust verification of sender legitimacy, making it significantly harder for attackers to impersonate trusted domains. Artificial intelligence and machine learning systems continuously analyze email patterns and user behavior to identify suspicious activities and potential phishing attempts in real-time. Web browsers now incorporate built-in phishing protection features that check websites against regularly updated databases of known malicious URLs. Multi-factor authentication serves as a critical backup measure, ensuring that even if phishing credentials are compromised, attackers cannot gain unauthorized access without additional verification steps. Security information and event management (SIEM) systems aggregate and correlate data from multiple sources to detect and respond to phishing campaigns across an organization's entire network infrastructure.

4.1.1 AI-Powered detection

Machine learning algorithms have revolutionized phishing detection by analyzing email content and metadata in real-time (Polakis et al. 2012). These systems can identify subtle patterns in text, images, and sender behavior that might escape traditional rule-based filters. By continuously learning from new attack patterns, AI-powered solutions adapt to emerging threats and improve their detection accuracy over time. The algorithms examine multiple factors simultaneously, including language patterns, sender reputation, and attachment characteristics, to make nuanced decisions about email legitimacy. Natural Language Processing (NLP) models can now detect social engineering attempts by analyzing the emotional manipulation and urgency in message content, providing

an additional layer of sophistication to threat detection. Deep learning networks excel at identifying phishing sites that use slight visual modifications or character substitutions to mimic legitimate websites, catching even highly sophisticated impersonation attempts. Transfer learning techniques allow AI systems to apply knowledge gained from known phishing patterns to identify novel attack variations, significantly reducing the time needed to detect new threats. Modern AI systems can analyze network traffic patterns and user behavior in real-time to identify potential command-and-control communications associated with successful phishing attacks. The integration of computer vision algorithms enables detection of manipulated brand logos and website layouts, effectively catching sophisticated visual spoofing attempts that traditional systems might miss.

4.1.2 Email authentication

Email authentication protocols like DMARC, SPF, and DKIM form a critical foundation of modern email security (Murphy 2018). These protocols work in concert to verify the authenticity of email senders and protect against domain spoofing. SPF verifies that emails originate from authorized sending servers, while DKIM ensures message integrity through cryptographic signatures. DMARC builds upon these protocols by providing clear policies for handling authentication failures and enabling domain owners to monitor potential abuse of their domains. Together, these protocols significantly reduce the likelihood of spoofed emails reaching their intended targets. The implementation of BIMI (Brand Indicators for Message Identification) extends these protections by allowing organizations to display verified logos in email clients, providing visual confirmation of sender legitimacy. Advanced reporting capabilities within DMARC enable organizations to gain visibility into email authentication failures and attempted spoofing attacks, facilitating rapid response to emerging threats. The integration of these protocols with modern cloud email services provides seamless protection across hybrid environments, ensuring consistent security regardless of email infrastructure. Time-based One-Time Password (TOTP) systems can be incorporated into the authentication chain to provide additional verification for high-risk email transactions or sensitive communications. The development of quantum-resistant cryptographic algorithms ensures that these authentication protocols will remain secure even as quantum computing capabilities advance.

4.2 User Education and Awareness

Despite technological advances, human error remains a critical factor in successful phishing attacks. Proctor (2019) emphasizes the importance of comprehensive training programs that strengthen the human firewall against social engineering attempts. Interactive simulations provide hands-on experience in identifying suspicious emails and websites, allowing users to make mistakes in a safe environment. Regular phishing drills test employee vigilance and reinforce best practices by sending controlled phishing attempts throughout the organization. Real-world scenario training helps employees understand current attack techniques by analyzing recent incidents and emerging threats. Continuous assessment and feedback enables organizations to measure the effectiveness of their training programs and identify areas where additional education may be needed. This multi-faceted approach to security awareness creates a more resilient workforce capable of recognizing and responding appropriately to phishing attempts in their daily operations. Gamification elements incorporated into training programs increase engagement and knowledge retention by rewarding employees for correctly identifying phishing attempts and maintaining high security awareness scores. Microlearning modules delivered at regular intervals help combat security fatigue by breaking down complex topics into digestible segments that can be easily absorbed and remembered. Peer-to-peer learning networks within organizations enable employees to share their experiences with phishing attempts, creating a collaborative security culture where awareness becomes part of daily conversation. Role-specific training tailored to different departments addresses the unique phishing risks faced by various employee groups, from finance teams handling wire transfers to IT staff managing system access. Integration of behavioural psychology principles into training programs helps employees understand and resist the emotional manipulation tactics commonly used in social engineering attacks.

5. Future Directions

5.1 Advanced Detection Methods

Future anti-phishing solutions will likely incorporate more sophisticated detection methods powered by emerging technologies. Behavioral biometrics adds an extra layer of security by analyzing unique user patterns like typing rhythm, mouse movements, and interaction habits to identify suspicious deviations from normal behavior. Contextual authentication examines multiple environmental factors such as device location, time of access, and network characteristics to validate user identity. Real-time threat analysis continuously monitors

network traffic and email patterns to detect and respond to phishing attempts as they occur, rather than relying on static rules. Machine learning-based prediction models leverage historical attack data to recognize subtle patterns and anticipate new phishing tactics, enabling proactive defense measures before attacks can succeed.

These advanced detection methods work together to create a more robust security framework that can adapt to evolving threats while minimizing disruption to legitimate users. As phishing attacks become more sophisticated, these technologies will play an increasingly crucial role in maintaining effective cybersecurity defenses.

5.2 Integration of Blockchain Technology

Blockchain technology shows significant potential in strengthening anti-phishing defenses through its inherent security features. Immutable transaction records ensure that every interaction is permanently logged and cannot be altered, making it easier to detect and trace fraudulent activities. Decentralized authentication eliminates single points of failure by distributing identity verification across multiple nodes, reducing the risk of credential theft. Smart contract implementation automates security protocols and access controls, ensuring consistent enforcement of security policies without human intervention. Secure communication channels built on blockchain infrastructure provide end-to-end encryption and verification, making it significantly more difficult for attackers to intercept or manipulate sensitive communications.

These blockchain-based solutions create a more resilient security framework that could fundamentally change how organizations protect against phishing attempts while maintaining transparency and trust in digital interactions.

6. Conclusions and Recommendations

The evolution of phishing from simple email scams to sophisticated, AI-driven attacks reflects the dynamic nature of cybersecurity threats. As Fielding and Taylor (2020) observe, the ongoing arms race between attackers and defenders necessitates continuous innovation in detection and prevention strategies. Looking ahead, organizations must prioritize both technological solutions and human-centered approaches, combining advanced detection systems with comprehensive security awareness training to create resilient defenses against evolving phishing threats.

The increasing sophistication of phishing attacks, particularly through AI and deepfake technologies, presents unprecedented challenges for organizations and individuals alike. As attackers continue to refine their methods, traditional security measures alone are no longer sufficient. A holistic defense strategy must incorporate multiple layers of protection, including advanced AI detection systems, blockchain-based authentication, and robust user education programs. Organizations should focus on developing adaptive security frameworks that can evolve alongside emerging threats while maintaining usability for legitimate users.

Furthermore, the human element remains crucial in phishing defense. Regular training and awareness programs must evolve beyond simple rule-based instruction to develop critical thinking skills that help users identify and respond to sophisticated social engineering attempts. Success in combating modern phishing threats will depend on organizations' ability to foster a security-conscious culture while leveraging the latest technological advances in threat detection and prevention.

References

Abu-Nimeh, S., Nappa, D., Wang, X. and Nair, S. (2007) 'A comparison of machine learning techniques for phishing detection', Proceedings of the eCrime Researchers Summit, pp. 60-69.

Emigh, A. (2005) 'Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures', ITTC Report on Online Identity Theft Technology and Countermeasures.

Fielding, R.T. and Taylor, R.N. (2020) 'Phishing in the cloud: A survey of the challenges and risks', Journal of Cloud Computing: Advances, Systems and Applications, 9(1), pp. 1-15.

Hasbini, H. (2021) 'IoT Security: Review, Blockchain Solutions, and Open Challenges', IEEE Internet of Things Journal, 8(1), pp. 1-11.

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

Jakobsson, M. and Myers, S. (2007) Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. John Wiley & Sons.

Kotzias, P., Moshchuk, A., Levchenko, D. and Chachra, N. (2019) 'The Rise of Malicious AI-Driven Phishing Attacks', IEEE Security & Privacy, 17(5), pp. 6-11.

Marchal, S., Francois, J., State, R. and Engel, T. (2014) 'PhishStorm: Detecting Phishing With Streaming Analytics', IEEE Transactions on Network and Service Management, 11(4), pp. 458-471.

Moore, T. and Clayton, R. (2007) 'The impact of public information on phishing attack and defense', Proceedings of the 5th International Conference on Financial Cryptography and Data Security, pp. 66-82.

Murphy, K.R. (2018) 'The effect of phishing training on employee susceptibility: A research study', Journal of Information Technology Management, 29(3), pp. 51-65.

Polakis, M., Ioannidis, S. and Markatos, E.P. (2012) 'Collaborative phishing detection and prevention: Building the next generation security infrastructure', IEEE Security & Privacy, 10(6), pp. 31-38.

Proctor, S. (2019) 'Enhancing phishing awareness: A study on effective training strategies', Journal of Cybersecurity Education, Research and Practice, 4(1).

Ramzan, Z. and Atkinson, J.W. (2012) 'A phisher's tale: Understanding the threat of spear phishing', Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 23-25.

Rivest, R.L. (2010) 'Spear phishing: A wake-up call for internet security', IEEE Security & Privacy, 8(3), pp. 1-2.

Westerlund, M. (2019) 'The emergence of deepfake technology: A review', Technology Innovation Management Review, 9(11), pp. 39-52.