

The Effect of Artificial Intelligence of the Development of Phishing Attacks

Dr. Sadam Mohammad Awaishah

Assistant Professor of Administrative Law, Public Law Department, Faculty of Law, Al-Ahliyya Amman University, Amman, Jordan, Email: s.awaishah@ammanu.edu.jo, ORCID: <https://orcid.org/0000-0003-1984-8530>

Dr. Suzan Mamdouh Al-Awaysheh, Lawyer and Legal Advisor, Independent Researcher, Email:

dr.suzanawaysheh@gmail.com, ORCID: <https://orcid.org/0009-0009-4508-0757>

Dr. Salah Mohammed Awaishah, Assistant Professor of Law, Private Law Department, Faculty of Law, Applied Science Private University, Amman, Jordan, Email: s_alawaesheh@asu.edu.jo, ORCID: <https://orcid.org/0009-0000-0800-4231>

Dr. Tawfiq Khashashneh, Assistant Professor, Faculty of Law, Applied Science Private University Amman, Jordan, Email: t_khashashneh@asu.edu.jo, ORCID: <https://orcid.org/0009-0001-2104-3654>

Dr. Karimeh Jalal Bqoor, Assistant Professor of Civil Law, Faculty of Law, Amman Arab University, Amman, Jordan, Email: karimeh@aaau.jo, ORCID: <https://orcid.org/0009-0006-0677-5669>

Dr. Ayman Asfour, Part-Time Lecturer, Faculty of Law, Al-Ahliyya Amman University Amman, Jordan, Email: asinjlawi2000@yahoo.com, ORCID: <https://orcid.org/0009-0007-8949-3700>

Dr. Wasfi Mahmoud Masoud Al-Khraisat, Assistant Professor of Administrative Law, Public Law Department, Faculty of Law, Al-Ahliyya Amman University, Amman, Jordan, Email: w.alkhraisat@ammanu.edu.jo, ORCID: <https://orcid.org/0000-0002-4573-5129>

Abstract

Phishing is considering one of the most dangerous cyber crimes in the digital date, as it poses a direct threat to individuals and institutions and sap trust in cyber space. The study objective to analyze the relationship between the development of AI technologies and phishing crime. The study adopted a descriptive-analytical methodology based on a review of relevant scientific literature and international reports addressing this phenomenon. The finding revealed that artificial intelligence has significantly contributed to the evolution of phishing methods through the automation of fraudulent message generation, the enhancement of linguistic quality. In addition, AI-powered technologies such as voice phishing and visual phishing using deep fake techniques have increased the sophistication of phishing attacks and made their detection more complex. The study confirmed that AI also served as an effective tool of the protection information's and strengthening cyber security by the use of machine learning algorithms to detect phishing patterns, analyze behavioral anomalies, and consolidate early threat identification. And it recommended the importance of balancing the risks and benefits of AI technologies through adoption robust legal frameworks and advanced cyber security strategies, and protecting digital services.

Keywords: Phishing, Artificial Intelligence, Cyber crime, Cyber security, Electronic Public Administration, Legal Responsibility.

1. Introduction

The modern world is witnessing a rapid digital transformation that has reshaped the patterns of work and the provision of services in both the public and private sectors. (Schmitt & Flechais, 2024) The transformation has been driven by the widespread adoption of electronic platforms for delivering governmental and commercial services.

Despite the numerous advantages offered by these digital advancements, they have created a fertile environment for the proliferation of cyber crimes, leading to fundamental changes in their nature and complexity. (Kumar et al., 2024)

Among these, electronic phishing is considered one of the most dangerous and widespread cyber crimes. It commonly exploits human trust to gain unauthorized access to sensitive information. (Alqahtani et al., 2025)

Recent international reports Europol (2024) indicate that phishing represents one of the most prevalent cyber crimes worldwide, serving as a primary entry point for numerous cyber attacks targeting both institutions and individuals

The accelerated development of phishing attacks is closely linked to advances in artificial intelligence (AI) technologies. Contemporary studies shown that large language models and deep learning techniques have improved the accuracy and persuasiveness of fraudulent messages, making their detection more challenging compared to traditional methods (Akhtar & Rawol, 2024).

Organizational analyses have reported that hackers' use of AI to customize phishing messages based on user data has led to changes in attack quality and increased success rates (Parti, Dearden, & Choi, 2023).

In this context, cyber security requires advanced tools and techniques to address these evolving threats, especially the defensive application of AI technologies. (Kumar et al., 2024) Recent studies have indicated that AI-supported detection systems, which utilize predictive analysis and automated learning, have demonstrated higher capabilities in identifying abnormal attacks early and reducing response times compared to traditional signature-based methods (Sarfraz et al., 2025).

As well, electronic public administration plays a pivotal role in mitigating phishing risks by implementing policies, organizational frameworks, and digital security infrastructures capable of monitoring and preventing cyber attacks. (Alqahtani et al., 2025)

International reports OECD (2024) confirm that integrating e-government systems into national cyber security strategies enhances response capabilities and reduces the impact of cyber attacks on critical services

Finally, cyber crime legislation serves a fundamental role in addressing phishing, through marginalization of electronic fraud, organization of criminal investigations, and strengthening cross-border judicial cooperation. (Jabir et al., 2025)

Modern legal studies Council of Europe (2024) and UNODC (2024) highlight that continuous updates of national and international legislation enhance law enforcement capacities to pursue cyber criminals and collect digital evidence, thereby increasing deterrence and limiting the spread of such crimes.

The study sleeked to statement the impact of artificial intelligence on the development of electronic phishing attacks, examine the role of technological advancements in strengthening cyber security against these attacks, and highlight the contributions of e-government and cyber crime legislation in mitigating risks and protecting digital services.

2. What is phishing?

2.1 Concept of Phishing

Phishing is defining as : " One of the forms of electronic crime that aims to deceive users and induce them to disclose sensitive information, such as passwords, banking card data, or personal information, and the typically carried out through impersonating trusted entities,

such as banks, government institutions, or technology companies" (Parti et al., 2023). This reliance on apparent institutional authority has a private-law analogue in ostensible agency, where legal consequences can turn on a third party's reliance on an appearance of authority; phishing weaponizes a technologically fabricated appearance without creating genuine agency (Alfawaer et al., 2023).

In involvement this type of crime, attackers often rely on different digital communication channels, such as email, text messages, fake websites, and social media platforms, and these attacks exploit weaknesses in users' cyber security awareness and their lack of vigilance when interacting with digital content (Csongor & Tóth, 2024).

A notable recent example occurred in 2025, when a phishing attack targeted a real estate company in New York City. In this incident, a major property management firm lost approximately \$19 million after receiving a fraudulent email impersonating the Battery Park City Authority. As a result, financial transfers were mistakenly made to a fraudulent bank account before the fraud was detected and federal investigations were initiated. This case highlights the severe risks associated with impersonation-based phishing attacks and their direct impact on the financial security of institutions (New York Post, 2025).

2.2 Types of Phishing

Phishing methods differ according to the level of targeting and the technologies used, which include the following:

2.2.1 Traditional Phishing

Traditional phishing is considered one of the oldest and simplest forms of phishing attacks. It primarily relies on sending mass, generic messages to a large number of users without specific targeting, with the aim of deceiving as many victims as possible. (Jakobsson & Myers, 2024)

The messages are commonly delivered via email, text messages, or social media platforms, and they often appear to originate from trusted entities such as banks, telecommunications companies, or government institutions. (Sujatha & Ramesh, 2024)

The traditional phishing messages usually contain links to fake websites that closely mimic official websites, prompting users to enter sensitive information such as usernames, passwords, or payment card details. (Jabir et al., 2025)

In some cases, these messages may also include malicious attachments designed to infect the user's device with malware once opened. This malware can enable attackers to gain control over the device or steal stored data. (Alqaralleh, 2025)

The success of traditional phishing largely depends on social engineering techniques, as attackers exploit emotions such as fear, urgency, or temptation to pressure users into responding without verifying the credibility of the message. (Munyira et al., 2025)

Despite its relative simplicity compared to more advanced phishing techniques, traditional phishing remains an effective threat, particularly in environments that lack adequate cyber security awareness or advanced protection systems. (Sujatha & Ramesh, 2024)

2.2.2 Spear Phishing

Spear phishing represents a more advanced and dangerous form of phishing fraud. Unlike traditional phishing, it does not rely on random mass distribution; instead, it targets specific individuals or institutions using carefully collected personal or professional information (Shahzad & Aman, 2024).

This information may include victims' names, job positions, professional relationships, or details related to their workplace, which makes the fraudulent messages appear more credible and convincing. (Europol, 2024)

Spear phishing attacks rely heavily on the collection and analysis of data from multiple sources, such as social media platforms, official institutional websites, or previous data breaches. (Ataih Albishri & Dessouky, 2024)

This information is then used to craft messages that appear to originate from reliable entities, such as direct managers, business partners, or official institutions. (Sharma & Goyal, 2025) And these messages often contain urgent or sensitive requests intended to pressure the victim into taking immediate action without verifying the authenticity of the message. (Mansoor & Iliev, 2025)

Recent studies indicate that spear phishing has significantly higher success rates compared to traditional phishing, due to its personalized approach and exploitation of professional and personal trust (Alqaralleh, 2025).

This type of attack is widely used to target government and financial institutions and often serves as an entry point for larger cyberattacks, such as internal system breaches or the theft of sensitive data. (Akhtar & Rawal, 2024)

2.2.3 Phishing by Text Messages (Smishing)

Phishing by short text messages, commonly referred to as Smishing, is considered one of the most dangerous forms of phishing fraud. This is primarily due to the widespread use of smart phones and the increasing reliance of users on text messaging to complete daily transactions. (Ataih Albishri & Dessouky, 2024)

Smishing attacks are typically carried out by sending short messages that appear to originate from trusted entities, such as banks, telecommunications companies, or government institutions. These messages often contain malicious links or urgent requests, such as prompts to update banking account details or verify suspicious transactions. (Schmitt & Flechais, 2024)

This type of phishing relies heavily on creating a sense of urgency and anxiety in the victim. (Ahmed et al., 2025) Messages are carefully crafted to suggest an immediate threat, such as account suspension, the imposition of fines, or the promise of rewards, which pressures users to respond quickly without verifying the authenticity of the message. (Shahzad & Aman, 2024) When the victim clicks on a malicious link or opens an attachment, they may be redirected to fake websites designed to steal personal or financial information, or malware may be installed on the victim's mobile device. (AlKhatatneh, 2023)

Recent international reports indicate that smishing attacks have significantly increased in recent years, particularly due to the difficulty of distinguishing fraudulent text messages compared to email-based phishing. Additionally, the limited deployment of advanced protection mechanisms in some telecommunications networks has contributed to the growing threat. (Ataih Albishri & Dessouky, 2024)

Smishing attacks have become increasingly sophisticated with the use of artificial intelligence technologies to generate and personalize messages according to the characteristics of targeted victims, thereby enhancing their effectiveness and posing a serious risk to cybersecurity (Europol, 2024; UNODC, 2024).

2.2.4 Voice Phishing (Vishing)

Voice phishing, commonly known as Vishing, relies on live telephone calls as the primary method for deceiving victims. (Shahzad & Aman, 2024) In these attacks, the attacker impersonates a trusted entity, such as a banking institution, a government agency, or a service provider, with the objective of persuading the victim to disclose sensitive information. Such information may include bank account numbers, verification codes, or personal data, exploiting the trust associated with real-time voice interaction (Mansoor & Iliev, 2025).

The evolution of vishing has become particularly evident in recent years due to the use of artificial intelligence and voice deep fake technologies, which enable attackers to accurately mimic the voices of legitimate employees or senior officials. (Ahmed et al., 2025) This significantly increases the credibility of fraudulent calls and makes it more difficult for victims to distinguish between genuine and fake communications. Moreover, data analysis technologies are employed to identify the most responsive targets and to craft persuasive scenarios tailored to the victim's professional or personal context. (Shahbazi et al., 2025)

Recent studies suggest that AI-supported vishing represents one of the most dangerous forms of phishing fraud, owing to its reliance on live human interaction and the exploitation of authority and urgency. (Shahzad & Aman, 2024) These factors result in higher success rates compared to text-based or email-based phishing methods. Consequently, vishing poses an increasing challenge to cyber security systems and necessitates advanced technical, organizational, and legal responses to mitigate its associated risks (Mansoor & Iliev, 2025).

2.2.5 Email Phishing

Email phishing is one of the most widespread and impactful forms of cybercrime in the digital era. It involves sending fraudulent email messages that appear to originate from trusted individuals or institutions. (Sharma & Goyal, 2025) The primary objective of these messages is to deceive users into disclosing sensitive information, such as passwords, bank account numbers, or credit card details, or to directly induce them to transfer funds (Akhtar & Rawol, 2024).

This type of phishing targets both individual users and organizations. Emails may be directed at specific individuals, known as spear phishing, or sent broadly to large groups in what is referred to as mass phishing. (Shahbazi et al., 2025) Attackers commonly rely on digital identity impersonation techniques, such as using legitimate company logos, spoofed email addresses, and professionally worded messages to gain the trust of recipients.

Email phishing messages may also contain malicious links or attachments that lead to data theft or the installation of malware on victims' devices. (Shahzad & Aman, 2024)

Furthermore, the methods employed in email phishing continue to evolve with advancements in artificial intelligence, enabling the generation of highly convincing and personalized messages that significantly increase the likelihood of successful attacks (Parti et al., 2023).

The prevalence of email phishing poses serious threats to the cyber security of individuals and institutions, resulting in substantial financial losses and undermining trust in digital communications. (Sharma & Goyal, 2025) Therefore, understanding the mechanisms of email phishing is a fundamental step toward developing effective detection and prevention strategies, whether through technological solutions or enhanced cyber security awareness programs. (Shahzad & Aman, 2024)

2.2.6 Phishing by Social Media and Chat

Social media phishing has emerged as one of the fastest-growing forms of cybercrime due to the widespread adoption of social media platforms such as Facebook, Instagram, and Twitter and their increasing use for both personal and professional communication. (Yerkebay

et al., 2024) This type of phishing typically involves creating fake accounts or compromising legitimate accounts to contact victims through private messages or public comments, often impersonating trusted entities or individuals familiar to the victim (Akhtar & Rawol, 2024).

Attackers exploit publicly available personal information on users' social media accounts, such as interests, social relationships, and professional profiles, to craft highly persuasive fraudulent messages. (Sharma & Goyal, 2025) These messages often include malicious links, urgent requests for transferring funds, downloading fake applications, or sharing verification codes. They leverage the informal and rapid-response nature of social media interactions to increase the likelihood of user compliance. (Jha, 2025)

A recent incident illustrates the risks associated with social media phishing. In 2025, a woman in India, a doctor, and fell victim to a fake WhatsApp message impersonating a bank and threatening to close her account. After clicking the malicious link, a fraudulent application was installed on her device, granting attackers access to her banking information and enabling multiple unauthorized transactions, resulting in direct financial losses (The Times of India, 2025). This case highlights the dangers of phishing and its reliance on exploiting trust in everyday digital applications.

The use of artificial intelligence has further intensified the threat posed by social media phishing. (Jha, 2025) AI tools can analyze user data to create fraudulent content that matches the writing style and social context of the victim and AI-powered chat bots can engage in continuous, persuasive interactions. International reports indicate that social media phishing is increasingly employed in digital fraud operations, particularly targeting youth and small organizations, posing growing challenges for cyber security systems (Europol, 2024; Akhtar & Rawol, 2024).

3. AI-Powered Phishing

In contrast to traditional phishing, AI-powered phishing leverages artificial intelligence and automated learning technologies to create highly personalized phishing messages based on the analysis of users' digital data and online behavior (Akhtar & Rawol, 2024). These methods can generate emails or text messages that appear extremely natural, significantly reducing the likelihood of detection compared to traditional phishing attacks. (Sharma & Goyal, 2025).

AI techniques may also use deep fake technologies to create audio or video clips that mimic officials or trusted figures, thereby increasing the credibility of fraudulent messages and coercing users into disclosing sensitive information. (Aldossari, 2021).

Smart phishing relies heavily on predictive analysis to identify the most susceptible targets, improving both accuracy and efficiency compared to traditional phishing methods, though it requires advanced technical resources and in-depth knowledge of digital user data. (Sharma & Goyal, 2025).

The rapid evolution of AI technologies has qualitatively transformed phishing attacks, which no longer rely on random, poorly constructed messages but instead demonstrate high levels of professionalism and precision, increasing both their success rates and the difficulty of detection. AI contributes in several key aspects:

- 1. Message Construction:** AI enables cybercriminals to generate linguistically flawless messages that simulate natural human style and are highly persuasive. (Alqaralleh, 2025) By analogy, legal scholarship on multilingual arbitration shows that linguistic proficiency can materially affect perceived fairness and procedural legitimacy, which helps explain why

linguistically polished AI-generated messages can be more persuasive to targets (Alhasan, 2025c).

2. Content Personalization: AI tailors phishing content based on the analysis of victims' digital behavior, including social media interactions, professional activities, and patterns of electronic service usage, thereby increasing the likelihood of user engagement. (Mansoor & Iliev, 2025)

3. Communication Style Simulation: AI can replicate the traditional communication style of institutions, including language, tone, and official formatting, enhancing the credibility of phishing messages and making it more difficult for victims to distinguish between legitimate and fraudulent content. (Akhtar & Rawol, 2024) A related account of linguistic due process treats language as constitutive of procedural justice rather than a neutral communication channel; in phishing, the same communicative force is inverted to manufacture authenticity and trust (Alhasan & Burr, 2025).

4. Audio-Based Attacks: AI-powered deep fake technologies allow attackers to replicate voices of real employees or officials with high accuracy, making voice phishing attacks particularly dangerous by exploiting trust and authority during live interactions. (Mansoor & Iliev, 2025)

Overall, AI has not only improved cyber security defense tools but has simultaneously escalated the sophistication and scale of phishing threats. (Yerkebay et al., 2024). For example, Akhtar and Rawol (2024) reported that cybercriminals used an advanced linguistic model to craft fraudulent messages targeting employees of a financial company, producing highly accurate messages in style and personal context, which resulted in the theft of funds.

4. Threats of Phishing Attacks

Phishing represents a live and multidimensional threat that affects various aspects of digital, social, and economic security. Consequently, its consequences are severe across multiple levels, as outlined below:

4.1 Cyber security for Institutions and Banks

Phishing is often the initial entry point in many sophisticated cyber attacks. Attackers commonly target employees, exploiting weaknesses in institutional defenses before later accessing internal systems. Studies have shown that a significant portion of data breaches begins with phishing emails that lead to the theft of login credentials, granting attackers access to sensitive systems. (Olaniyi & Adeyemo, 2025) The integration of artificial intelligence in phishing campaigns further increases the persuasiveness of fraudulent messages, making traditional cyber security measures insufficient on their own.

A notable case is *Experi-Metal, Inc. v. Comerica Bank* (2011), which involved an employee receiving a fraudulent email claiming to be from the bank requesting a login update. Once the credentials were entered, the attackers executed fraudulent transfers within hours, causing significant financial losses. The court examined the extent of the bank's liability for failing to detect suspicious activity in a timely manner.

4.2 Financial Stability for Individuals and Organizations

Phishing poses a serious threat to financial security at both individual and institutional levels. For individuals, successful phishing messages can lead to the theft of payment card information or access to financial accounts, resulting in direct financial losses that may only be discovered after the fraud occurs (Ghani et al., 2024).

Recent reports indicate a rise in phishing via text messages and messaging applications, where fake links purporting to be from banks are sent to users. (Al-Khraisat, et al. 2025) Clicking these links may install malware or steal banking information, leading to direct financial losses. This trend illustrates the adaptation of phishing techniques to everyday digital behavior (APWG, 2024).

At the institutional level, phishing attacks targeting employees or customers can result in substantial financial losses, including fraudulent transfers, legal and compensation costs, and diminished trust in the organization. For example, the 2019 phishing incidents targeting Facebook and Google involved a perpetrator impersonating a legitimate supplier and sending fraudulent invoices, resulting in over \$100 million being transferred to fraudulent accounts before detection. (US Department of Justice, 2019)

4.3 Digital Privacy

Phishing attacks often lead to the violation of users' personal data privacy, enticing victims to enter sensitive information on fake websites or through deceptive communications. Such breaches can expose users to identity theft, compromise email accounts, and reveal personal location or financial data, which may then be exploited for scams or digital surveillance. (Alqaralleh, 2025)

A prominent example is the Avalanche phishing network, which carried out thousands of email attacks impersonating well-known financial institutions and job portals. In one year alone, the group recorded more than 84,000 attacks, accounting for over half of all phishing incidents during that period (APWG, 2024; Wikipedia, 2024).

4.4 Trust in Digital Services

Trust is a fundamental factor in the adoption of digital services, especially in online banking, e-commerce, and government digital platforms. Exposure to successful phishing attacks can significantly reduce user trust, leading individuals to limit or abandon the use of such services. (Ghani et al., 2024).

This erosion of trust negatively impacts digital transformation efforts and hinders economic growth in the digital economy. Studies indicate that decreased trust results in resistance to adopting digital services, slowing technological progress for both institutions and countries (Saeed & Qureshi, 2025).

Phishing also serves as a gateway for more severe attacks, such as ransom ware and account hacking (UNODC, 2024). For instance, the 2020 Twitter account hacking incident involved attackers targeting company employees to access sensitive administrative tools. This attack led to the takeover of public figures' accounts, posting fraudulent tweets soliciting crypto currency, and generating illicit profits. The incident highlights the impact of phishing on widely used digital platforms and its effect on digital trust. (Federal Bureau of Investigation, 2020)

5. Confronting Phishing Attacks Using Artificial Intelligence Technologies

With the increasing use of AI in the development of phishing attacks, institutions and cyber security authorities have also adopted AI technologies to enhance detection, prevention, and response capabilities. (Hammed & Soyemi, 2023) Today, AI represents a fundamental pillar of modern cyber security strategies, providing the capacity to analyze massive amounts of data and detect abnormal patterns with greater speed and accuracy than traditional methods.

5.1 Analysis of Electronic Message Content and Detection of Suspicious Patterns

AI employs natural language processing (NLP) and machine learning to analyze the content of electronic messages, including linguistic features, structure, and style. These technologies can identify indicators of phishing, such as urgent expressions, unusual instructions, or deviations from normal communication patterns within institutions. Studies have demonstrated that intelligent AI models are capable of detecting phishing messages with significantly higher accuracy compared to rule-based systems (Sarfranz et al., 2025).

5.2 Automatic Detection of Malicious Links and Fake Websites

AI contributes to cyber security by analyzing links and website addresses included in electronic messages. This involves examining domain features, site behavior, and historical activity, and comparing them with known threat databases. (Purwadi, et al., 2025) AI mechanisms can identify fake websites early, including newly constructed sites not yet listed in blacklists, reducing the success rate of phishing attacks (Microsoft, 2024).

5.3 Predictive Analysis for Anticipating Phishing Campaigns

Predictive analytics is one of the most prominent applications of AI in cyber security. And through analyzing historical attack data, attacker behavior, and previous campaign timings, AI can predict potential phishing waves, identify vulnerable categories or sectors, and allow proactive preventive measures before attacks occur. (ENISA, 2024)

5.4 User Training via Virtual Phishing Simulations

In addition to technical solutions, AI is used to enhance human cyber security awareness through realistic virtual phishing simulations. (Purwadi, et al., 2025) These training programs adapt to user behavior and skill level, improving the ability to detect fraudulent messages in real environments. Recent studies confirm that interactive AI-based training significantly reduces the success rates of phishing attacks within institutions (OECD, 2024).

5.5 The Strategic Role of Artificial Intelligence in Cyber security

AI is not merely a defensive tool but has become a pivotal element in building smart and proactive cyber security systems to confront phishing attacks. (Hammed & Soyemi, 2023) Its effectiveness relies on the integration of technological solutions, legal frameworks, and human awareness, achieving a sustainable balance in combating advanced electronic crimes. Studies confirm that AI-based systems markedly reduce phishing success rates (Sarfranz et al., 2025).

Recent research further indicates that the integration of AI has significantly enhanced phishing detection. AI-based models, particularly ensemble and machine learning approaches, have demonstrated high effectiveness in identifying phishing attempts (Alsariera et al., 2024; Ataih et al, 2024). In social media environments, AI improves the detection of deceptive content and mitigates phishing risks (Sharma & Goyal, 2025).

In other way, generative AI has transformed social engineering tactics, increasing the sophistication and credibility of phishing messages (Schmitt & Flechais, 2024). These findings underscore the critical role of artificial intelligence in combating phishing threats in the digital age. (Hammed & Soyemi, 2023)

6. Role of e-Government in Strengthening Protection against Phishing Attacks.

The fight against phishing attacks is not limited to AI technology solutions. It requires an inclusive approach to leaving sensitive information and critical infrastructure vulnerable to ever-growing cyber threats (Schmitt & Flechais, 2024).

E-Government, primarily participates in protecting digital services and strengthening national cyber security (Figuerola et al., 2025). This indicates that effective digital governance

is a decisive element in reducing the risks of cyber crime and strengthening trust in electronic services (OECD, 2024).

6.1 Unification of Cyber security Standards for Digital Government Services.

E-Government contributes to the unification of standards for information security and data protection on Government platforms, including policies for identity verification, traffic management, and data encryption (Figueroa et al., 2025). This system helps reduce security gaps that can be exploited by criminals using phishing or identity theft against Government entities or targeting users of their digital services (ENISA, 2024).

6.2 Strengthening Multi-Factor Authentication (MFA) Systems.

Multi-factor authentication systems are essential for government entities to function effectively and widely. Implementing MFA systems within official electronic services limits the impact of phishing attacks to the leakage of login data. (Awaisheh, 2025)

Modern reports confirm that multi-factor authentication increases the effectiveness of procedures for reducing information leaks resulting from phishing, which it seeks to implement robust and adaptable security measures to safeguard e-Government services and citizens' data. (Microsoft, 2024).

6.3 Nationalist Digital Identity Management

Nationalist digital identity systems are based on the e-Government strategy to limit phishing, enabling the verification of the credibility of users of official entities, and reducing the need to access links, and electronic messages that are primarily exploited in operations (Stone, 2022).

As Governments adopt information and communication technologies to implement e-Government, they become more vulnerable to cyber threats, which can compromise sensitive information and citizens' privacy (Stone, 2022). Modern studies demonstrate that digital identity systems contribute to increasing confidence in the security of electronic transactions (World Bank, 2024). Comparable research on digital contract administration identifies blockchain and smart contracts as tools for improving transparency, automation, and transaction security, while recognizing implementation costs and complexity (Alhasan, 2025d). More specifically, permissioned blockchain records have been proposed to strengthen immutability, cryptographic authentication, and evidentiary reliability, offering an adjacent design logic for trusted digital-service records and verification architectures (Alhasan, 2026b).

6.4 Coordination with the Computer Emergency Response Team (CERT)

This contributes to the coordination between the E-Government and the computer emergency response team in the early monitoring of phishing campaigns, (Sharma & Goyal, 2025). The security of information exchange and the issuance of official alerts for users, strategic cyber security Governance are essential to ensure that protection measures are implemented effectively and that a culture of security is promoted across all levels of Government (Figueroa et al., 2025). This coordination is essential to reducing the spread of attacks and limiting their effects on the digital infrastructure (UNODC, 2024).

6.5 Digital Awareness Campaigns.

E-government plays a role assumes that is fundamental for disseminating cyber security awareness during official campaigns targeting citizens and employees. The modern research to increase security awareness and directly reduce the success rates of fraudulent phishing attacks, especially those that rely on social engineering (OECD, 2024).

6.6 Integration with legal and organizational frameworks.

E-government works to integrate technological solutions with the organization's laws for the digital space, with regard to the protection of personal data against electronic crime. (Stone, 2022). This integration contributes to strengthening legal deterrence, improving security compliance, and supporting institutional cooperation in the fight against cross-border cybercrime. (Council of Europe, 2024)

And it is clear that the role of e-government in combating fraudulent phishing goes beyond protection technology. It includes direct integration of digital governance, trust building, institutional coordination, and legal integration (Stone, 2022). And this is the complementary element for artificial intelligence technologies, and it contributes to the construction of integrated cyber security systems capable of countering advanced threats in the modern digital environment. (Al-Khraisat, et al. 2025)

7. Legal Liability in AI-Backed Phishing Crimes

The growing use of artificial intelligence technologies in phishing attacks has significantly complicated the process of establishing legal liability, whether for criminal perpetrators or for entities that may be indirectly responsible for the resulting harm. (Kail et al., 2023) Traditional legal frameworks are increasingly inadequate in addressing these crimes, given their reliance on automation, machine learning, and the involvement of third-party technological infrastructures. These developments challenge conventional notions of intent, causation, and accountability. (Akhtar & Rawol, 2024).

7.1 Criminal Liability of Perpetrators

AI-backed phishing crimes extend beyond traditional forms of cybercrime due to their heightened level of complexity, scalability, and organizational sophistication. Criminal liability primarily attaches to individuals or legal entities that design, deploy, control, or direct intelligent systems for the purpose of committing criminal acts, including at the stage of automated execution. (Hossain et al., 2023)

Contemporary legal scholarship emphasizes that the use of artificial intelligence does not exempt offenders from criminal responsibility. On the contrary, it may justify enhanced penalties, reflecting both the dangerous nature of the technological tools employed and the magnitude of the harm caused (UNODC, 2024).

Data from the Internet Crime Complaint Center (IC3), affiliated with the Federal Bureau of Investigation (FBI), indicate that thousands of phishing-related fraud incidents are reported annually. However, in many cases, perpetrators cannot be identified or prosecuted due to the use of fabricated digital identities distributed across multiple jurisdictions. One notable case involved a mid-sized U.S. company in which an employee received a fraudulent email impersonating a trusted business partner. This deception resulted in the unauthorized transfer of funds to external accounts. Despite an official investigation, neither the perpetrators could be traced nor the funds recovered, as the attack relied on foreign servers and intermediary bank accounts located outside U.S. jurisdiction (FBI-IC3, 2023).

This case highlights the substantial challenges faced by law enforcement agencies in combating phishing crimes, particularly in the absence of effective and timely international cooperation. (Kail et al., 2023) Moreover, advanced technologies designed to conceal digital identities undermine traditional deterrence mechanisms, reinforcing the urgent need for preventive technical safeguards and adaptive legislative responses.

7.2 The Problem of Identifying Actors in AI-Backed Crimes

A central legal challenge in AI-backed phishing crimes is the difficulty of attribution. When autonomous or semi-autonomous AI models are used to generate messages, select

victims, or adapt attack strategies, identifying the responsible human actor becomes increasingly complex. This issue has prompted significant debate within legal systems regarding the appropriate allocation of responsibility. (Ghani et al., 2024)

Recent legal approaches emphasize the concept of “human control” or “human oversight,” whereby liability is assigned to the party that exercises effective control or direction over the AI system (Hossain et al., 2023). Under this framework, responsibility may fall on developers, operators, or end users, depending on their role and capacity to influence the system’s behavior (Council of Europe, 2024). The same insistence on identifiable human responsibility appears in arbitration scholarship, where auxiliary assistance must not displace the arbitrator’s core decisional functions and undisclosed involvement becomes legally significant when it penetrates those functions (Alhasan, 2026a). Applied by analogy, AI automation should not obscure the human actor who directs, supervises, or materially controls a phishing operation.

7.3 Civil Liability for Damages

In addition to criminal liability, AI-backed phishing attacks give rise to civil liability for the financial and moral damages suffered by victims. Such liability includes compensation for individuals and organizations affected by financial losses, data breaches, or reputational harm. (Awaishah et al., 2025b).

In the context of artificial intelligence, civil liability may also extend to entities that fail to implement adequate preventive measures. (Kail et al., 2023). These include digital service providers, financial institutions, or organizations that neglect to adopt appropriate cyber security standards and risk mitigation protocols (European Union, 2024).

7.4 Responsibility of Developers and Suppliers of Artificial Intelligence Technologies

The legal debates have increasingly focused on the responsibility of developers and suppliers of AI systems in cases, where their technologies are abusing for phishing and other cyber crimes. (Aawisheh, Al-Hassan, & Mansour, 2024; Awaishah, 2025).

Modern legislation, particularly within the European Union, has clarified this issue through regulatory instruments such as the EU Artificial Intelligence Act. The framework emphasizes the obligation of AI developers to take on to principles of "safe-by-design" and "prevention of misuse", requiring them to incorporate risk mitigation measures during the design, development, and deployment of AI systems. (Ghani et al., 2024)

However, contemporary legal standards do not impose automatic criminal liability on developers or technology providers solely because their systems are misused for criminal purposes. (Obaid, 2025). Criminal responsibility arises only where there is demonstrable negligence, lack of due diligence, or intentional collusion in facilitating the unlawful use of the technology (European Parliament, 2024).

Conversely, cyber security firms have advanced sophisticated machine learning algorithms capable of analyzing email content and detecting phishing messages with increasing accuracy. These technological advancements necessitate that organizations and individuals adopt more advanced cyber security measures alongside updated legislative strategies to address evolving threats. (Lysenko et al., 2024)

Recent studies indicate that AI-powered phishing attacks are becoming progressively more difficult to detect using traditional security systems, thereby underscoring the need for continuous innovation in both technical defenses and regulatory responses (Akhtar & Rawol, 2024).

7.5 The Role of National and International Laws in Combating Phishing

For the given the inherently transnational nature of phishing crimes, which often cross multiple jurisdictions within seconds, the importance of international cooperation and the harmonization of legal frameworks have become increasingly evident (Norris & Mateczun, 2023). Comparable transnational dispute settings likewise show that fragmented jurisdiction, inconsistent procedural standards, and sovereignty concerns can impede coordinated legal responses (Alhasan, 2025a). In phishing cases, those coordination problems are intensified because perpetrators, infrastructure, victims, and evidence may be located in different states.

And the international agreements, most notably the Budapest Convention on Cyber crime, provide a foundational legal basis for criminalizing phishing activities, facilitating cross-border cooperation, enabling the exchange of digital evidence, and supporting the extradition of offenders. (Kail et al., 2023)

Recent reports emphasize the urgent need to modernize these legal frameworks to adequately account for technological developments associated with artificial intelligence and automated cyber crime techniques (Europol, 2024).

A growing body of legal scholarship has examined the regulatory and proprietarily challenges posed by phishing crimes. Research suggests that many existing cyber crime laws lack explicit provisions addressing phishing, thereby creating gaps in legal accountability and enforcement (Purwadi, et al., 2025). In the Indonesian context, scholars have highlighted the necessity of clearer and more specific legislative provisions, as well as the practical difficulties of prosecuting phishing offenders under general cyber crime statutes (Lokapala, et al., 2025; Sari, 2025). Cross-domain legal analysis also demonstrates that vague or poorly structured legal instruments can generate disputes over scope, sequence, and enforceability, whereas objective criteria and precise drafting improve predictability (Alhasan, 2025b). For phishing legislation, that lesson supports clearer definitions of prohibited conduct, attribution standards, and liability triggers.

Similar enforcement challenges arise in addressing online marketplaces that trade phishing tools and malicious links. Legal analysts question whether current electronic information and transaction laws are sufficient to deter such activities effectively (Irawati & Kunarso, 2025). Legal effectiveness also depends on the quality of adjudicative reasoning: Jordanian arbitration scholarship shows that insufficient reasoning may undermine the validity of a legal decision (Alhasan, 2024). Although the doctrinal setting differs, AI-assisted cybercrime cases likewise require reasoned findings on intent, causation, control, and evidentiary attribution.

Comparative legal studies further reveal that fragmented regulatory frameworks, such as those found in Tanzania, struggle to define and penalize phishing offenses adequately, drawing attention to more comprehensive legislative models, such as Nigeria's cyber crime laws, as potential benchmarks (Shelimo, 2025).

Studies indicate that many local governments lack adequate cyber security frameworks to counter such threats, particularly in terms of policy adoption and technical preparedness. (Norris & Mateczun, 2023) The distinction between formal legal reform and effective implementation has also been documented in other areas of Jordanian law, where inconsistent interpretation and enforcement can limit the practical effect of protective legislation (Al-Zubi et al., 2024). The same distinction matters for anti-phishing legislation, which requires operational enforcement capacity in addition to statutory coverage.

The rapid evolution of phishing attacks has been closely linked to advances in artificial intelligence technologies. These attacks increasingly rely on automation and machine learning to personalize fraudulent messages and evade detection systems. (Hossain et al., 2023)

Furthermore, the absence of harmonized international cyber security standards has exacerbated vulnerabilities across jurisdictions, highlighting the need for coordinated legal and technical responses (Awaisheh et al., 2025).

Additionally, research on statutory limitations demonstrates that certain computer crime acts fail to fully capture the deceptive and manipulative nature of phishing tactics, thereby limiting their effectiveness in addressing AI-enhanced cyber deception (Thonraweewong, 2025).

8. Conclusion

The study examined phishing as one of the most prevalent and impact forms of cyber crime in the digital date. Phishing depend primarily on deceiving users and persuading them to expose sensitive information through the impersonation of trusted entities. Quick advancements in AI technologies have drove to a radical transformation in phishing methods, deepening the relationship between artificial intelligence and cyber crime and imposing increasing challenges on cyber security systems (Parti et al., 2023).

AI function a significant role in the development of phishing attacks by the automation of fraudulent message creation and the enhancement of their linguistic and contextual quality. Forward language models are capable of producing highly realistic messages that are free of grammatical errors and tailored to the digital behavior and personal characteristics of victims.

The significantly increases the success rates of phishing attacks and makes their detection more difficult.(Akhtar & Rawol, 2024) AI also facilitates the expansion of targeted phishing campaigns (spear phishing), in which individuals or institutions are selectively targeted based on detailed data that are automatically collected and analyzed.

On the other hand, the development of deep fake technologies has strengthened audio-visual phishing attacks. By impersonating the voices or images of officials or employees, attackers are able to convince victims to execute financial, bargain or disclose confidential information. Studies signalize that this form of AI-supported phishing represents a serious threat to digital trust, as it becomes increasingly difficult for ordinary users to distinguish between genuine and manipulated content.

Reciprocally, AI is also exercised as an effective tool in combating phishing and enhancing cyber security. New protection systems rely on machine learning algorithms to resolve email patterns, detect malicious links and counterfeit websites, and identify abnormal behaviors that may signalize pressing attacks. (Csongor & Tóth, 2024) Predictive analytics more reserved enable the identification of attack patterns from previous incidents, allowing institutions to anticipate potential phishing campaigns and implement contemplate measures before they occur (Sarfraz et al., 2025).

The study existence of a dynamic and interactive relationship between the development of AI and cyber crime and its impact on cyber security. So AI become criminals to innovate more sophisticated phishing techniques, it together provides cyber security systems with intelligent tools for detection and response.

The dual-use nature confirms that AI constitutes a double-edged weapon that requires effective legal regulation, strong technical governance, and increased cyber security awareness among users to lessen the risks of phishing. The standardization of processes and adoption of advanced technologies will enable quicker and more effective incident responses.

The dual-use nature confirms that AI constitutes a double-edged weapon that requires effective legal regulation, strong technical governance, and increased cyber security

awareness among users to lessen the risks of phishing. The standardization of processes and adoption of advanced technologies will enable quicker and more effective incident responses.

Also, the study demonstrates that legal responsibility for AI-supported phishing crimes operates at multiple levels, including criminal liability for perpetrators, civil liability for damages suffered by victims, and organizational responsibility for developers and operators of intelligent systems. Updating legislation and strengthening international cooperation are therefore essential to ensure effective legal deterrence and robust cyber security protection in the digital date. While promoting a security culture and encouraging citizen participation will contribute to a safer and more resilient cyberspace.

8.1 Recommendations

1. Updating legal legislation to keep pace with AI-supported phishing crimes, including deep fake-based phishing and targeted spear phishing.
2. Establishing regulatory frameworks that impose preventive responsibilities on developers and operators of artificial intelligence systems to mitigate misuse in cybercrime.
3. Strengthening reliance on artificial intelligence technologies within cyber security systems to enhance early detection and prediction of phishing attacks.
4. Intensifying cyber security awareness and training programs to educate users about modern phishing techniques and reduce their success rates.
5. Supporting international cooperation and information sharing to address the cross-border nature of phishing crimes.
6. Conducting specialized studies that examine the legal and cyber security dimensions of phishing fraud in the context of artificial intelligence.

References

- Aawisheh, S., Al-Hassan, T., & Mansour, A. (2024). The status of digital evidence in administrative litigation. *Al-Balqa Journal for Research and Studies*, 27(3), 42–55. <https://doi.org/10.35875/pgdx2798>
- Ahmed, S., Sumra, I. A., Khan, I., & Abdullah, H. (2025). A comprehensive review on the role of AI in phishing detection mechanisms. *Journal of Computing & Biomedical Informatics*, 8(02). <https://doi.org/10.XXXX/jcbi.2025.8.02.861>
- Akhtar, M., & Rawol, R. (2024). Advances in AI-powered phishing attacks. *Journal of Cybersecurity Studies*, 12(3), 45–62.
- Akhtar, Z. B., & Rawol, A. T. (2024). Harnessing artificial intelligence for cybersecurity: Challenges, opportunities, risks, and future directions. *Computing and Artificial Intelligence*, 2(2), 1485. <https://doi.org/10.59400/cai.v2i2.1485>
- Alfawaeer, A. M., Alhasan, T. K., & Alfaoury, A. M. (2023). Ostensible agency in Jordanian civil law: An in-depth scrutiny of juridical frameworks and the imperative for legislative reformulation. *Relacoes Internacionais no Mundo Atual*, 4(42), 810–831. <https://doi.org/10.21902/Revrima.v4i42.6566>
- Alhasan, T. K. (2024). The devil is in the details: An analysis of the criteria for adequate reasoning in arbitral awards in Jordan. *Conflict Resolution Quarterly*, 41(3), 357–361. <https://doi.org/10.1002/crq.21412>

- Alhasan, T. K. (2025a). Arbitration in the era of trade wars: Balancing sovereignty and global commerce. *Social Sciences and Humanities Open*, 12, Article 101945. <https://doi.org/10.1016/j.ssaho.2025.101945>
- Alhasan, T. K. (2025b). From pathology to precision: Transforming multi-tiered dispute resolution clauses in international contracts. *Conflict Resolution Quarterly*, 42(4), 557–563. <https://doi.org/10.1002/crq.21473>
- Alhasan, T. K. (2025c). Linguistic proficiency disclosures in international arbitration: Enhancing fairness and efficiency. *International Journal for the Semiotics of Law*, 38(5), 1805–1827. <https://doi.org/10.1007/s11196-025-10261-4>
- Alhasan, T. K. (2025d). The role of blockchain in modernizing FIDIC contracts: Opportunities and challenges. *Studies in Systems, Decision and Control*, 234, 565–573. https://doi.org/10.1007/978-3-031-84636-6_49
- Alhasan, T. K. (2026a). Arbitral secretaries and the validity of awards: A doctrinal and case law-based evaluation of challenges based on undisclosed assistance. *Arbitration International*, 42(1), 119–131. <https://doi.org/10.1093/arbint/aiaf020>
- Alhasan, T. K. (2026b). Blockchain-enhanced construction records: Transforming evidentiary standards and dispute resolution in international arbitration. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 18(2), Article 04526011. <https://doi.org/10.1061/JLADAH.LADR-1467>
- Alhasan, T., & Burr, A. (2025). Beyond words: Ensuring due process in multilingual arbitrations. *International Journal for the Semiotics of Law*, 38(7), 2219–2241. <https://doi.org/10.1007/s11196-025-10278-9>
- Al-Khraisat, W. M. M., & et al. (2025). The extent to which recourse to arbitration is permissible in the settlement of disputes arising under procurement contracts. *Journal of Human Security*, 21(1), Article 03. <https://doi.org/10.12924/johs2025.210103>
- AlKhatatneh, A. (2023). Legal regulation of diplomatic immunities and privileges. *Al-Balqa Journal for Research and Studies*, 26(1). <https://doi.org/10.35875/1105-026-001-002>
- Aldossari, M. Z. (2021). A survey on phishing attacks in cyberspace. *International Journal of Computer (IJC)*, 41(1), 46–58. <https://doi.org/10.53896/ijc.v41i1.1902>
- Alqahtani, A., Alshammari, M., & Alzahrani, S. (2025). AI-driven phishing detection: Enhancing cybersecurity with reinforcement learning. *Journal of Cybersecurity and Privacy*, 5(2), 26. <https://doi.org/10.3390/jcp5020026>
- Alqaralleh, B. (2025). Phishing attacks: Trends, techniques, and mitigation strategies. *Journal of Cybersecurity Research*, 9(1), 45–60.
- Alsariera, Y. A., Alanazi, M. H., Said, Y., & Allan, F. (2024). An investigation of AI based ensemble methods for the detection of phishing attacks. *Engineering, Technology & Applied Science Research*, 14(3), 14266–14274. <https://doi.org/10.48084/etasr.7267>
- Al-Zubi, J. K., Maaqqbeh, M., Awaisheh, S. M., Mofleh, Y. A., Awaisheh, S. M., & Alhasan, T. K. (2024). Progress and challenges in the legal framework of women's rights in Jordan. *International Journal of Criminal Justice Sciences*, 19(1), 519–531. <https://doi.org/10.5281/zenodo.19128>
- Anti-Phishing Working Group. (2024). *Phishing activity trends report*. APWG.

- Ataih Albishri, A., & Dessouky, M. M. (2024). A comparative analysis of machine learning techniques for URL phishing detection. *Engineering, Technology & Applied Science Research*, 14(6), 18495–18501. <https://doi.org/10.48084/etasr.8920>
- Awaishah, S. M. (2025). From paper to pixels: The legal status and challenges of electronic writing in administrative contracts. A comparative study of current legal systems. *Electronic Government*, Article 2025. <https://doi.org/10.1504/EG.2025.144726>
- Awaishah, S. M., Alsaraireh, N., Alkasasbeh, A. A. M., & Odeibat, M. A. (2025). The extent to which recourse to arbitration is permissible in the settlement of disputes arising under procurement contracts. *Journal of Human Security*, Article 2025. <https://doi.org/10.12924/johs2025.210103>
- Awaishah, S. M. A., Al-Abbadi, H. S., Al-Dabbas, N. A., Hmaidan, R., Al Khalaileh, L., Awaishah, S. M., & Al Tarawneh, A. S. (2025). New claims and causes of action before the Court of Appeal in Jordanian civil procedure. *Journal of Human Security*, Article 2025. <https://doi.org/10.12924/johs2025.210108>
- Council of Europe. (2024). *Artificial intelligence and criminal liability in cybercrime*.
- Council of Europe. (2024). *Cybercrime and electronic evidence: Legal challenges in the AI era*.
- Csongor, H., & Tóth, D. (2024). Artificial intelligence in cybersecurity: Examining liability, crime dynamics, and preventive strategies. *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 8, 730–747. <https://doi.org/10.25234/eclic/32299>
- ENISA. (2024). *Artificial intelligence and cybersecurity: Threat landscape and defensive applications*. European Union Agency for Cybersecurity.
- European Parliament. (2024). *EU Artificial Intelligence Act: Legal framework and implications*.
- European Union. (2024). *Civil liability rules for artificial intelligence systems*.
- Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA)*.
- Experi-Metal, Inc. v. Comerica Bank, 2011 U.S. Dist. LEXIS 27609 (E.D. Mich. Mar. 18, 2011).
- Federal Bureau of Investigation. (2020). *Public service announcement: Cryptocurrency fraud*. FBI.
- Federal Bureau of Investigation, Internet Crime Complaint Center. (2023). *Internet crime report 2023*. FBI.
- Figuerola, V., Sánchez Crespo, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2025). Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals. *International Journal of Information Security*, 24, Article 121. <https://doi.org/10.1007/s10207-025-01024-0>
- Ghani, U., Shahzad, M., & Ahmad, R. (2024). Financial impacts of phishing attacks on organizations: Evidence from emerging economies. *Journal of Financial Crime*, 31(5), 1024–1040. <https://doi.org/10.1108/JFC-12-2023-0182>

- Hammed, M., & Soyemi, J. (2023). Classification of phishing attacks in social media using associative rule mining augmented with firefly algorithm. *GPH International Journal of Computer Science and Engineering*, 6(6), 1–10. <https://doi.org/10.5281/zenodo.8059093>
- Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2023). Local government cybersecurity landscape: A systematic review and conceptual framework. *Applied Sciences*, 14(13), 5501. <https://doi.org/10.2139/SSRN.4680227>
- Irawati, H. P., & Kunarso. (2025). Enforcement of laws against the sale of phishing links for the purpose of personal data theft based on the ITE Law. *YURIS: Journal of Court and Justice*, 3(4), Article 802. <https://doi.org/10.56943/jcj.v3i4.802>
- Jabir, R., Le, J., & Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. *AI*, 6(8), 174. <https://doi.org/10.3390/ai6080174>
- Jakobsson, M., & Myers, S. (2024). *Phishing and countermeasures: Understanding the increasing threat*. Wiley Cybersecurity Series.
- Jha, A. (2025). Phishing forensics: A systematic approach to analyzing mobile and social media fraud. *Journal of Cyber Security*, 7, 109–134. <https://doi.org/10.32604/jcs.2025.064429>
- Kail, E., Banati, A., Fleiner, R., Mosavi, A., & Mako, C. (2023). In *Proceedings of the 2023 IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics*.
- Kumar, S., Menezes, A., Giri, S., & Kotikela, S. (2024). What the phish! Effects of AI on phishing attacks and defense. In *Proceedings of the International Conference on AI Research*. <https://doi.org/10.34190/icair.4.1.3224>
- Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2025). Aspek yuridis kejahatan phishing dalam ketentuan hukum di Indonesia. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*. <https://doi.org/10.18196/ijclc.v5i1.19853>
- Lysenko, S., Liubchenko, A., Kozakob, V., Demianchuk, Y., & Krutik, Y. (2024). Global cybersecurity: Harmonising international standards and cooperation. *Multidisciplinary Review*. <https://doi.org/10.31893/multirev.2024spe021>
- Mansoor, N., & Iliev, A. I. (2025). Explainable AI for DeepFake Detection. *Applied Sciences*, 15(2), 725. <https://doi.org/10.3390/app15020725>
- Mansoor, S., & Iliev, R. (2025). AI-driven spear phishing: Emerging threats and mitigation. *Cybersecurity Journal*, 11(1), 12–30. <https://doi.org/10.1016/cyberj.2025.01.002>
- Microsoft. (2024). *Cyber signals: AI and the evolution of phishing threats*.
- Microsoft. (2024). *Cyber signals: The role of MFA in preventing phishing attacks*.
- Munyira, A., Patel, R., & Singh, V. (2025). Exploiting the human element: AI-driven phishing and multivector attacks. *International Journal of Computer Applications*, 187(56). <https://doi.org/10.5120/ijca2025925974>
- New York Post. (2025). NYC real estate firm allegedly scammed out of \$19 million after phishing email impersonating Battery Park City Authority. *New York Post*.
- Norris, D. F., & Mateczun, L. K. (2023). Adoption of cybersecurity policies by local governments: 2020. *Journal of Cybersecurity Education, Research and Practice*, 2023(2).

- OECD. (2024). *Digital government and trust in the age of artificial intelligence*.
- OECD. (2024). *Strengthening digital security and trust in the age of artificial intelligence*.
- Obaid, F., & Alougili, M. (2025). Jordanian diplomacy and food security during the COVID-19 lockdowns: A case study. *Al-Balqa Journal for Research and Studies*, 28(2).
<https://doi.org/10.35875/5wvbm193>
- Olaniyi, O. S., & Adeyemo, A. B. (2025). The role of phishing in security breaches: Institutional vulnerabilities and defense mechanisms. *International Journal of Information Security Science*, 14(2), 85–103.
- Parti, A., Sharma, P., & Kumar, S. (2023). Phishing in the age of artificial intelligence: Threats and countermeasures. *International Journal of Information Security*, 18(2), 101–118.
- Parti, K., Dearden, T., & Choi, S. (2023). Understanding the use of artificial intelligence in cybercrime. *International Journal of Cybersecurity Intelligence & Cybercrime*, 6(2).
<https://doi.org/10.52306/2578-3289.1170>
- Purwadi, P., Makhfud, M., & Jamaludin, A. (2025). Legal accountability and policy gaps in social engineering based phishing cybercrimes. *Research Horizon*, 5(3), 797–806.
<https://doi.org/10.54518/rh.5.3.2025.580>
- Saeed, A., & Qureshi, S. (2025). Digital trust and phishing: How cyber fraud affects user confidence in e-services. *Journal of Cyber Behavior & Trust*, 2(1), 14–29.
- Sarfraz, M., Sumra, I. A., Khalid, B., & Fatima, E. (2025). AI-driven predictive threat detection and cyber risk mitigation: A survey. *Journal of Computing & Biomedical Informatics*, 8(02), 103–118.
- Sari, R. M. P. (2025). Criminal responsibility in cybercrime: An analysis of phishing crimes in Indonesia. *JHK: Jurnal Hukum dan Keadilan*, 2(5), Article 418.
<https://doi.org/10.61942/jhk.v2i5.418>
- Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, 57, Article 324.
<https://doi.org/10.1007/s10462-024-10973-2> Springer
- Shahbazi, Z., Jalali, R., & Molaeevand, M. (2025). AI based phishing detection and student cybersecurity awareness in the digital age. *Big Data and Cognitive Computing*, 9(8), 210.
<https://doi.org/10.3390/bdcc9080210>
- Shahzad, T., & Aman, K. (2024). Unveiling the efficacy of AI based algorithms in phishing attack detection. *Journal of Informatics and Web Engineering*, 3(2), 116–133.
<https://doi.org/10.33093/jiwe.2024.3.2.9>
- Sharma, V., & Goyal, M. K. (2025). AI-driven techniques for detecting and preventing social media phishing attacks. *Revista Electronica de Veterinaria*, 25(2), Article 1889.
<https://doi.org/10.69980/redvet.v25i2.1889>
- Shelimo, H. H. (2025). Strengthening Tanzania's legal framework against phishing attacks: Lessons from Nigeria. *East African Journal of Law and Ethics*, 8(1), Article 3936.
<https://doi.org/10.37284/eajle.8.1.3936>

Stone, A. G. (2022). The role risk-management plays in reducing insider threat's in the federal government. *Information Security Journal: A Global Perspective*, 31(3), 338–345.
<https://doi.org/10.1080/19393555.2021.1998735>

Sujatha, R., & Ramesh, G. (2024). A systematic review of deep learning techniques for phishing email detection. *Electronics*, 13(19), 3823.
<https://doi.org/10.3390/electronics13193823>

The Times of India. (2025). Doctor duped in online phishing scam, loses ₹82,010 after clicking fake bank link. *The Times of India*.

Thonraweewong, K. (2025). Legal limitations relating to the application of Thai computer-related crime Act to the case of “Phishing”. *Kasem Bundit Journal*.

U.S. Department of Justice. (2019). *Lithuanian man pleads guilty to wire fraud involving Google and Facebook*. United States Department of Justice.

UNODC. (2024). *Cybercrime prevention and criminal justice responses*. United Nations Office on Drugs and Crime.

Wikipedia. (2024). Avalanche (phishing group). *Wikipedia, The Free Encyclopedia*.
[https://en.wikipedia.org/wiki/Avalanche_\(phishing_group\)](https://en.wikipedia.org/wiki/Avalanche_(phishing_group))

World Bank. (2024). *Digital public infrastructure and cybersecurity governance*.

Yerkebay, A., Yubuzova, K., & Seitkaliyeva, Z. (2024). Social networks as an attack vector for targeted attacks. *Computing & Engineering*, 2(1), 14–18.
<https://doi.org/10.51301/ce.2024.i1.03>