MODERN METHODS OF DETECTING AND COUNTERING PHISHING ATTACKS IN THE DIGITAL ENVIRONMENT

UDC: 004.056.53
DOI: https://doi.org/10.53486/tids2025.10

OLHA HABORETS
PhD, Associate Professor
Department of Operational and Investigative Activities and Information Security
Faculty No. 3, Donetsk State University of Internal Affairs, Ukraine
ORCID ID: 0000-0001-7791-6795

LUDMILA RYBALCHENKO
PhD, Associate Professor
Department of Cyber Security and Information Technologies
University of Customs and Finance, Dnipro, Ukraine
luda_r@ukr.net
ORCID ID: 0000-0003-0413-8296

Abstract. Phishing attacks have evolved into a major cybersecurity threat, leveraging advanced technologies and human vulnerabilities to achieve unauthorized access, data exfiltration, and financial exploitation. This article explores the transformation of phishing tactics, identifies the latest detection technologies including artificial intelligence and behavioral analysis, and evaluates the strategic countermeasures adopted across various digital sectors. Through a comprehensive review of modern techniques such as Natural Language Processing, threat intelligence sharing, and multi-factor authentication, the article emphasizes the importance of an adaptive and collaborative approach to phishing defense.

Hackers use deception to lure users out of their account passwords and compromise personal information, creating a threat to the confidentiality of information. With phishing attacks, which are a common form of digital threats to accounts, attackers hack into accounts using hypertext links with malicious codes. The issue of phishing attacks is one of the of the most common methods of gaining access to confidential user data. With the growth of information technology comes the development of various technologies for creating phishing attacks that are related to messaging and mobile devices. Attackers often intercept and crack codes to gain access to accounts and create a cyberattack using malware. Often, fraudsters use phishing attacks to gain access to accounts and sell the data to criminals. Data breaches for large enterprises can become the basis for various cyberattacks, which can result in the loss of large amounts of money.

Keywords: phishing, cyber threats, artificial intelligence, behavioral biometrics, Natural Language Processing, social engineering, threat intelligence, cybersecurity strategy, phishing detection, phishing mitigation.

JEL Classification: H56, D80.

INTRODUCTION

Phishing remains one of the most sophisticated and persistent threats in the contemporary digital landscape, evolving rapidly to exploit vulnerabilities in both human behavior and technological infrastructure. As digital communication and online services expand globally, cybercriminals continue to adapt phishing methodologies to bypass traditional security mechanisms,

often employing advanced social engineering tactics and automation. Consequently, the necessity for modern, integrated approaches to phishing detection and prevention has become a focal point in cybersecurity research and practice.

Phishing attacks have diversified significantly in recent years, moving beyond simplistic email-based scams to encompass more complex forms such as spear-phishing, smishing, vishing, pharming, and clone phishing. Each vector is designed to manipulate the target through various channels – email, SMS, voice calls, manipulated websites, or forged communications – to extract credentials, financial information, or other sensitive data. The polymorphic and context-aware nature of these attacks complicates detection and response, requiring a layered and adaptive defense strategy. Notably, attackers increasingly exploit current events, such as global pandemics or geopolitical conflicts, to increase the success rate of their campaigns.

MAIN CONTENT

1. Materials and Methods

Contemporary methods for phishing detection increasingly rely on the integration of artificial intelligence (AI) and machine learning (ML) algorithms. These technologies enable the continuous analysis of large volumes of data to identify subtle anomalies and predictive indicators of phishing behavior. Natural Language Processing (NLP) is applied to scrutinize the semantic and syntactic features of messages, detecting urgency, coercion, and deceptive intent commonly embedded in phishing content. Similarly, heuristic and signature-based systems continue to serve as foundational elements, particularly for recognizing known patterns of malicious activity.

Advanced phishing detection systems now combine AI-driven threat modeling with real-time data feeds, enabling predictive analytics and early warnings. Sandboxing techniques are also employed to isolate suspicious attachments and observe their behavior in a controlled environment. Email security gateways equipped with anomaly detection mechanisms can effectively intercept phishing emails before they reach end-users. Furthermore, phishing simulators are widely used to test employee readiness and improve organizational response mechanisms.

Another crucial aspect of modern phishing mitigation is the use of URL and domain analysis, which assesses the trustworthiness of links based on registration data, structural characteristics, and real-time comparisons with threat intelligence databases. Browser extensions and endpoint security software further augment this analysis by providing real-time alerts and blocking access to flagged content. Behavioral biometrics represents a promising frontier, enabling systems to detect fraudulent access attempts based on deviations in user interaction patterns, such as typing rhythms or mouse dynamics. Coupled with geolocation data and device fingerprinting, these methods can create robust authentication profiles.

To counter phishing effectively, organizations must adopt a proactive and holistic approach. Multi-factor authentication (MFA) serves as a vital line of defense, reducing the risk of unauthorized access even when credentials are compromised. Concurrently, comprehensive security awareness training fosters a culture of vigilance among employees, enhancing their ability to identify and report suspicious communications. The implementation of email authentication protocols – such as SPF, DKIM, and DMARC – significantly curtails email spoofing, reinforcing trust in organizational correspondence.

2. Results and Discussion

Moreover, the integration of threat intelligence sharing mechanisms across sectors facilitates a collaborative response to emerging phishing campaigns. Platforms for real-time exchange of indicators of compromise (IOCs) and attack signatures empower security teams to anticipate and neutralize threats with greater efficiency. This collective intelligence, when augmented with automated analytics, provides a scalable defense framework adaptable to the evolving tactics of threat actors. International cooperation, including joint initiatives by governmental and private cybersecurity organizations, further strengthens global resilience.

Nevertheless, significant challenges persist. Adversaries are increasingly leveraging AI to enhance the believability of phishing messages and to automate the customization of attacks based on publicly available personal data. As a result, defensive systems must evolve beyond static rule sets to incorporate dynamic, self-learning capabilities capable of anticipating novel attack vectors. Future research should prioritize the development of context-aware detection models, interdisciplinary strategies combining human cognition with machine reasoning, and regulatory frameworks that mandate transparent data sharing and accountability.

CONCLUSIONS

In conclusion, the dynamic and multifaceted nature of phishing necessitates a strategic fusion of technological innovation, informed policy-making, and continuous education. Modern countermeasures – when applied coherently – can substantially reduce the effectiveness of phishing campaigns and fortify the resilience of digital ecosystems against exploitation. The path forward lies in the collaborative advancement of intelligent systems that not only detect threats but also preemptively disrupt adversarial operations in the cyberspace continuum. As digital environments continue to expand, so too must our capacity to protect them through adaptive, ethical, and intelligent cybersecurity practices.

The increasing complexity of cyberspace presents a profound challenge to achieving cyber resilience, exacerbating inequities that leave less-resourced organizations vulnerable. Geopolitical tensions are prompting organizations to re-evaluate their strategies, balancing security concerns with global operations. Such tensions often drive targeted attacks, as state-sponsored actors exploit vulnerabilities for espionage and disruption. This dynamic landscape requires adaptive strategies that account for shifting global risks and supply chain dependencies.

REFERENCES

1. Haborets, O. A. (2024). The impact of cyber threats on community and citizen security: Analysis and perspectives on resolution. In Interaction between state bodies and the public in counteracting criminal offenses in the central regions of Ukraine: Roundtable materials (April 17, 2024, Kropyvnytskyi) (pp. 36–37). Kropyvnytskyi: DonDUVS. Access mode: https://dnuvs.ukr.education/wp-content/uploads/2024/06/zbirnyk_ materialiv_kruglogo_stolu_ord_ta_ib-2.pdf
2. Global Cybersecurity Outlook 2025. World Economic Forum. 2025. p. 49. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf