Cybersecurity and Law

2026 Nr 1(15)

DOI: 10.35467/cal/220501

Cybersecurity of the contemporary information society

Cyberbezpieczeństwo współczesnego społeczeństwa informacyjnego

ppłk dr inż. Bartłomiej TEREBIŃSKI
Akademia Sztuki Wojennej
ORCID: 0000-0002-6124-9905
E-mail: b.terebinski@akademia.mil.pl

Abstract

The purpose of this article is to describe the nature of contemporary cyber threats and their social consequences, as well as to ensure the security of the information society in cyberspace. The analyses focus on digital identity, threats to network users, and both mobile and stationary devices in use. The activities related to the discussion of factual material and the systematization of conclusions from the conducted scientific considerations were made possible by the use of selected theoretical research methods. Analysis and synthesis allowed for the decomposition of the studied cyberthreats into their component elements, allowing for the identification of their essence and the diagnosis of the relationship between them and users functioning in the information society. Today's cyberthreats are increasingly advanced and dynamic, requiring organizations and cybersecurity professionals to continually refine their defense tools and strategies. The use of behavioral analytics allows for the detection of anomalies in system and user behavior, allowing for faster response to potential attacks, while AI-based mechanisms enable automated threat detection and adaptive adjustments to security measures to new attack vectors. Investing in raising user awareness and competence is fundamental. Regular training helps raise awareness of threats such as phishing and social engineering, and also teaches best practices such as creating strong passwords and using password managers. A security culture that prioritizes these threats minimizes the risk of errors and increases the organization's resilience to attacks.

Keywords

information society, online presence, cyber hygiene, e-identity, digital profile

Streszczenie

Celem niniejszego artykułu jest opisanie istoty współczesnych cyberzagrożeń i ich konsekwencji społecznych oraz zapewnienia bezpieczeństwa społeczeństwa informacyjnego w cyberprzestrzeni. Podejmowane analizy koncentrują się wokół tożsamości cyfrowej, zagrożeń dla użytkowników sieci, jak również urządzeń zarówno mobilnych jak i stacjonarnych będących w użytkowaniu. Działania związane z omówieniem materiału faktograficznego i usystematyzowaniem wniosków z przeprowadzonych rozważań naukowych były możliwe dzięki zastosowaniu

wybranych teoretycznych metod badawczych. Analiza i synteza pozwoliły na dekompozycję badanych zagrożeń cyberprzestrzeni na elementy składowe, co pozwoliło na identyfikację ich istoty oraz zdiagnozowanie związku między nimi a użytkownikami funkcjonującymi w społeczeństwie informacyjnym. Współczesne cyberzagrożenia są coraz bardziej zaawansowane i dynamiczne, co wymaga od organizacji oraz specjalistów od cyberbezpieczeństwa nieustannego doskonalenia narzędzi i strategii obronnych. Wykorzystanie analityki behawioralnej pozwala na wykrywanie anomalii w zachowaniu systemów i użytkowników, dzięki czemu można szybciej reagować na potencjalne ataki, natomiast mechanizmy oparte na sztucznej inteligencji umożliwiają automatyzację detekcji zagrożeń i adaptacyjne dostosowywanie zabezpieczeń do nowych wektorów ataku. Inwestowanie w podnoszenie świadomości i kompetencji użytkowników jest fundamentalne. Regularne szkolenia pomagają uświadomić zagrożenia, jak np. phishing czy inżynieria społeczna, a także uczą dobrych praktyk, takich jak tworzenie silnych haseł czy korzystanie z menedżerów haseł. Kultura bezpieczeństwa, która stawia je na pierwszym miejscu, minimalizuje ryzyko popełniania błędów i zwiększa odporność całej organizacji na ataki.

Słowa kluczowe

społeczeństwo informacyjne, obecność online, cyberhigiena, e-tożsamość, profil cyfrowy

Introduction

In the era of pervasive digital connectivity, cybersecurity has become a fundamental condition for ensuring the confidentiality, integrity, and availability of information. Technological progress has been accompanied by the rapid evolution of cybercriminal tactics, creating an increasingly complex threat environment for individuals, organizations, and governments. Among the most significant threats are malware[1], phishing campaigns[2], ransomware attacks[3], and zero-day exploits. These threats continue to increase in both scale and sophistication, frequently targeting critical infrastructure, healthcare systems, and commercial organizations. Artificial intelligence further transforms the threat landscape by enabling attackers to automate malicious activities, generate convincing phishing content, and develop adaptive malware capable of bypassing traditional defenses[4]. Consequently, organizations must adopt proactive security measures and continuously modernize their protective capabilities[5].

Effective cybersecurity requires a comprehensive infrastructure that combines technical, organizational, and procedural safeguards. Firewalls, intrusion detection and prevention systems, encryption mechanisms, and continuous monitoring solutions constitute essential elements of modern cyber defense. Frameworks such as those promoted by the National Institute of Standards and Technology (NIST)[6] provide structured approaches to risk management and incident response. Behavioral analytics and AI-supported

[1] https://www.fortinet.com/lat/resources/cyberglossary/types-of-malware0 [access 04.01.2026].
[2] R. Tanti, Study of Phishing Attack and their Prevention Techniques, „Interantional Journal Of Scientific Research In Engineering And Management" 2024, vol. 08, pp. 1-8.
[3] J. Jiang, J. Ross, G. Bai, Ransomware Attacks and Data Breaches in US Health Care Systems, "JAMA Network Open" 2025, vol. 8(5):e2510180, pp. 1-4.
[4] G. Blessing et al., The Emerging Threat of Ai-driven Cyber Attacks: A Review, „Applied Artificial Intelligence" (2022) vol. 36(1), p. 23.
[5] R. Kvyetnyy et al., Critical cybersecurity aspects for improving enterprise digital infrastructure protection, „IAPGOŚ" 2025, vol. 1, p. 69.
[6] https://www.nist.gov/cybersecurity-and-privacy (access 07.01.2026).

security systems further enhance detection capabilities and support predictive threat analysis. The aim of this study is to describe contemporary cyber threats affecting the information society by identifying their key characteristics and examining their impact on users functioning in digital environments.

Digital identity in the information society

In the digital age, creating and managing an online presence has become an essential element of both personal and professional identity. Individuals develop digital personas through social media activity, professional platforms, and everyday online interactions. At the same time, every action performed online contributes to a digital footprint that documents behavior and influences reputation. Understanding how digital identity is created and maintained is therefore crucial for navigating contemporary digital environments. The construction of an online identity is a continuous process involving the presentation of personal information, opinions, achievements, and interests. Platforms such as LinkedIn[7] facilitate professional self-presentation, while social media support broader forms of personal expression. The credibility of a digital identity depends largely on authenticity and consistency. Since online profiles frequently serve as a first point of contact for employers, colleagues, and institutions, their content can significantly affect professional and social opportunities. A digital footprint consists of the traces left by online activities, including posts, comments, search histories, and browsing behavior[8]. Unlike traditional communication, digital records often persist for extended periods and may remain accessible even after deletion. Consequently, past statements or actions can reappear unexpectedly and influence future opportunities. Effective management of a digital footprint requires regular monitoring of online content, careful use of privacy settings, and responsible sharing of information[9].

The persistence of online information creates significant challenges for privacy protection. Search engines, archives, and replicated databases frequently preserve information long after publication[10]. As a result, individuals may struggle to remove outdated or harmful content. This phenomenon highlights the importance of considering the long-term implications of online activity and reinforces the need for responsible digital behavior[11]. Privacy concerns have intensified as digital platforms collect, process, and commercialize increasing amounts of personal information. Data breaches, identity theft, and extensive behavioral profiling demonstrate the risks associated with large-scale data collection[12]. To mitigate these threats, users should employ strong passwords, enable two-factor authentication, and regularly review privacy settings. Balancing

[7] https://www.linkedin.com/home?originalSubdomain=pl (access 07.01.2026).
[8] I. Sharma, A. Aggarwal, Digital Footprints and the Battle for Data Sovereignty: Digital Privacy, Security, and Ownership, Driving Decentralization and Disruption With Digital Technologies, DOI: 10.4018/979-8-3693-3253-5.ch005 (access 02.01.2026).
[9] D. Hariyani, P. Hariyani, S. Mishra, The role of leadership in sustainable digital transformation of the organization, „Sustainable Futures" 2025, vol. 10, p. 101.
[10] S. Zannettou et al., Understanding Web Archiving Services and Their (Mis)Use on Social Media, „Proceedings of the International AAAI Conference on Web and Social Media" 2018, vol. 12(1), pp. 1-10.
[11] I. Ullah, R. Boreli, S. Kanhere, Privacy in targeted advertising on mobile devices: a survey, „International Journal of Information Security" 2022, vol. 22(12), pp. 647-678.
[12] X. Zhang, Data breach: analysis, countermeasures and challenges, „International Journal of Information and Computer Security" 2022, no. 9, p. 402.

the benefits of digital services with the protection of personal information remains one of the key challenges of the information society.

The right to be forgotten[13] has emerged as an important legal and ethical mechanism for strengthening individual control over personal data. This principle allows individuals to request the removal of information that is outdated, irrelevant, or harmful. Regulations such as the GDPR provide legal support for these requests, although implementation often involves balancing privacy rights against freedom of expression and public access to information. Consequently, debates regarding the scope and effectiveness of such rights continue across different jurisdictions. The governance of digital privacy depends on both legal regulations and platform policies. Social media services and search engines increasingly provide users with tools for managing visibility, deleting content, and controlling access to personal information. Nevertheless, differences in enforcement practices and commercial interests continue to generate controversy regarding the effectiveness of privacy protection measures.

Digital identity also has important psychological implications. Online environments frequently encourage idealized self-presentation and continuous comparison with others. Dependence on social validation through likes, comments, and followers may negatively affect self-esteem and mental well-being. In addition, the resurfacing of old content can generate embarrassment or anxiety, highlighting the emotional consequences of long-term digital visibility. Developing digital literacy and critical awareness therefore supports healthier engagement with online environments[14]. Emerging technologies, including artificial intelligence, blockchain[15], and advanced data analytics, will significantly influence the future of digital identity management. These technologies offer opportunities for greater personalization, security, and user control, but they also create new ethical challenges related to surveillance, data commodification, and individual autonomy. Responsible digital citizenship requires cooperation among users, organizations, and governments to ensure that technological innovation remains aligned with fundamental rights and social values.

In summary, digital identity management is a central component of contemporary participation in cyberspace. The persistence of digital footprints, privacy concerns, legal mechanisms such as the right to be forgotten, and the psychological consequences of online activity all influence how individuals function in digital environments. Effective management of these challenges requires digital literacy, responsible behavior, and an appropriate balance between technological innovation and the protection of individual rights.

User facing online threats

In contemporary digital environments, understanding cyber threats and maintaining proper cyber hygiene are essential for both individuals and organizations. As technology evolves, cybercriminals continuously develop new

[13] G. Mbah, Data Privacy and the Right to be Forgotten, „World Journal of Advanced Research and Reviews” 2022, vol. 16(02), pp. 1216-1232.

[14] S. Rane, The impact of social media on self-presentation and perception: navigating identity, communication, and connectivity in the digital age, https://www.researchgate.net/lab/Smita-Rane-Lab (access 30.12.2025).

[15] D. Hariyani et al., A literature review on transformative impacts of blockchain technology on manufacturing management and industrial engineering practices, „Green Technologies and Sustainability” 2025, vol. 3(3), p. 100.

methods to exploit vulnerabilities for financial gain, espionage, or disruption[16]. Consequently, awareness of cyber risks and responsible user behavior remain fundamental components of cybersecurity. Cyber threats include a broad range of malicious activities targeting the confidentiality, integrity, and availability of information systems[17]. Common examples include malware, phishing attacks, and unauthorized network intrusions. Malware, including ransomware and spyware, may encrypt data, steal information, or disrupt operations. Phishing campaigns use fraudulent messages to obtain credentials or financial information, while network intrusions exploit security weaknesses to gain unauthorized access. These threats originate from organized cybercriminal groups, malicious insiders, and vulnerabilities within third-party suppliers. Their consequences include financial losses, privacy violations, operational disruption, and reputational damage.

Cyber hygiene encompasses the routine practices that reduce exposure to cyber threats. Key measures include regular software updates, patch management, strong passwords, and multi-factor authentication (MFA). Unpatched systems remain vulnerable to known exploits, as demonstrated by incidents such as the WannaCry ransomware attack[18]. MFA significantly improves security by requiring additional identity verification beyond a password alone. Organizations that consistently implement these practices experience greater resilience and fewer security incidents. Although technological safeguards are important, users remain the first line of defense. Recognizing phishing attempts, verifying the legitimacy of communications, and avoiding suspicious links or downloads are essential behaviors. Prompt reporting of suspicious activity enables rapid investigation and mitigation. Security-awareness programs support these efforts by teaching employees how to identify and respond to cyber threats effectively. Protecting personal devices and home networks is equally important. Wireless networks should be secured using strong encryption protocols and unique passwords[19]. Antivirus and anti-malware solutions should be regularly updated to remain effective against emerging threats. Regular data backups provide an additional safeguard, enabling recovery from ransomware attacks, hardware failures, or accidental data loss.

Organizations must foster a culture of cybersecurity awareness through training, clearly defined policies, and continuous monitoring. Employees who understand phishing techniques, social-engineering methods, and secure data-handling practices are less likely to engage in risky behavior. Security policies provide consistent standards for password management, information handling, and incident response, while monitoring systems facilitate early threat detection. Maintaining effective cyber hygiene remains challenging due to the increasing sophistication of cyber threats. User complacency, limited awareness, and resource constraints often hinder the implementation of comprehensive security measures. Smaller organizations in particular may lack the financial and personnel resources required for advanced cybersecurity programs. These challenges emphasize that cybersecurity requires continuous adaptation,

[16] J. Thomas, A Case Study Analysis of the Equifax Data Breach 1 A Case Study Analysis of the Equifax Data Breach, 2019, DOI: 10.13140/RG.2.2.16468.76161 (access 04.01.2026).
[17] A. Tamrakar, B. Patra, Cybersecurity threats and countermeasures: a review, „Turkish Journal of Computer and Mathematics Education (TURCOMAT)" 2018, vol. 9(3), pp. 1400-1404.
[18] D. Singh, D. Parekh, T. Khandelwal, The WannaCry Attack: How it Worked and What We Learned, DOI: 10.13140/RG.2.2.19481.74084 (access 05.01.2026).
[19] D. Faíscas, (In)Security in Wi-Fi networks: a systematic review, „ARIS2 - Advanced Research on Information Systems Security" 2022, vol. 2(2), pp. 17-23.

investment, and commitment. Failure to meet cybersecurity responsibilities may result in severe consequences. Data breaches can expose sensitive information, generate substantial financial losses, damage organizational reputation, and lead to regulatory penalties[20]. Security incidents may also disrupt critical services and undermine stakeholder trust. Therefore, consistent security practices remain essential for both individuals and organizations. Continuous education and technological modernization are indispensable elements of cybersecurity. Regular training, awareness campaigns, and updates regarding emerging threats help maintain vigilance and reduce complacency. Simultaneously, organizations must modernize security tools and promptly address newly discovered vulnerabilities to ensure that protection mechanisms remain effective.

Password security represents a fundamental aspect of cyber hygiene. Strong passwords should be sufficiently long, unique, and composed of diverse character types[21]. Users should avoid predictable passwords and employ randomly generated credentials whenever possible. Because managing multiple complex passwords can be challenging, password managers provide a practical solution by securely storing credentials, generating strong passwords, and reducing password reuse across accounts[22]. The effectiveness of password protection increases when combined with best practices such as regular password updates, avoidance of credential reuse, and implementation of two-factor authentication. Selecting reputable password-management solutions[23] and periodically reviewing stored credentials further strengthens security. Together, these measures significantly reduce the risk of unauthorized access and credential compromise.

In conclusion, the growing complexity of cyber threats requires a comprehensive approach based on awareness, responsibility, and proactive security measures. Effective cyber hygiene, secure password management, user vigilance, and organizational support are essential elements of digital resilience. Through continuous education, technological modernization, and adherence to established security practices, individuals and organizations can significantly reduce cyber risk and maintain a secure digital environment.

Security of mobile and stationary devices on the network

In contemporary digital environments, ensuring the security of mobile and stationary devices has become a fundamental requirement for both individuals and organizations. As connectivity expands, cybercriminals continue to exploit vulnerabilities in devices and networks, making comprehensive protection strategies essential for safeguarding information and maintaining operational continuity. Mobile and stationary devices are exposed to numerous threats,

[20] A. Folorunso, Security compliance and its implication for cybersecurity, „World Journal of Advanced Research and Reviews" 2024, vol. 24(01), pp. 2105-2121.
[21] A. Shomope, A. Adeniyi, Enhancing Digital Security: A Comprehensive Review of Password Management Practices and Tools, „International Journal Of Mathematics And Computer Research" 2025, vol. 13(02), p. 4878.
[22] S. Armoogum et al., A Comprehensive Review of Cyber Hygiene Practices in the Workplace for Enhanced Digital Security, „JOIV International Journal on Informatics Visualization" 2025, vol. 9(1), p. 137.
[23] F.e. 2FA. J. Williamson, K. Curran, Best Practice in Multi-factor Authentication, „Semiconductor Science and Information Devices" 2021, vol. 3(1), p. 16.

including malware, unauthorized access, data theft, and physical loss[24]. Malware such as viruses, worms, spyware, and ransomware can compromise device integrity, steal information, or disrupt operations. Unauthorized access often results from weak passwords, phishing attacks, or other exploitation techniques that enable cybercriminals to gain control of systems and sensitive data. The theft or loss of devices further increases risk, particularly when adequate security mechanisms are absent. To address these threats, modern mobile devices incorporate advanced security features. Biometric authentication methods, including fingerprint and facial recognition technologies, provide effective user verification while maintaining convenience. Encryption protects data stored on devices and transmitted across networks, ensuring that information remains inaccessible to unauthorized parties. Remote wipe capabilities provide an additional layer of protection by enabling administrators or users to erase data from lost or stolen devices, reducing the likelihood of information leakage.

Stationary devices operating within organizational networks require comprehensive network-security measures. Firewalls serve as a primary defense mechanism by filtering network traffic and blocking malicious activity. Intrusion detection systems (IDS)[25] complement these protections by identifying suspicious behavior and facilitating rapid response. Virtual private networks (VPNs) protect remote communications by encrypting transmitted data, while regular software updates and patch management reduce exposure to known vulnerabilities[26]. Together, these measures establish a multilayered defense architecture that enhances the confidentiality, integrity, and availability of information resources.

Despite technological advances, maintaining device security remains challenging. Human error continues to represent one of the most significant vulnerabilities. Users frequently neglect software updates, reuse weak passwords, or fall victim to phishing campaigns and social-engineering techniques. Additionally, compatibility limitations and legacy systems may prevent organizations from implementing modern security solutions consistently across all devices. The continuous evolution of cyber threats further requires organizations to remain adaptable and proactive in their security strategies. Encryption plays a central role in protecting communications and stored information[27]. End-to-end encryption secures communications by ensuring that only authorized parties can access transmitted data. Similarly, storage encryption protects information against unauthorized access following theft or compromise. However, encryption alone cannot guarantee security. Weak key management, implementation flaws, and emerging attack techniques may reduce its effectiveness. Consequently, encryption must be integrated with broader security controls and regularly reviewed to ensure continued effectiveness.

---

[24] B. Duraisamy, A. Chakrabarti, D. Midhunchakkaravarthy, Smart Devices Threats, Vulnerabilities and Malware Detection Approaches: A Survey, „European Journal of Engineering and Technology Research" 2018, vol. 3(2), p. 7.

[25] L. Diana, P. Dini, D. Paolini, Overview on Intrusion Detection Systems for Computers Networking Security, „Computers" 2025, vol. 14(3), p. 210.

[26] K. Jyothi, I. Reddy, Study on Virtual Private Network (VPN), VPN's Protocols and Security, „International Journal of Scientific Research in Computer Science, Engineering and Information Technology" 2018, vol. 3(5), p. 923.

[27] S. Kumar et al., Secure data encryption key scenario for protecting private data security and privacy, „Journal of Discrete Mathematical Sciences and Cryptography" 2024, vol. 27(2), pp. 269-281.

Unsecured devices can introduce significant risks to organizational networks. Malware infections may spread across connected systems, while compromised devices can provide attackers with access to sensitive information. Data breaches, operational disruptions, and reputational damage frequently result from inadequate endpoint protection. These risks highlight the importance of combining device security, network protection, and user awareness within a unified cybersecurity strategy. Effective device security requires adherence to established best practices. Regular software updates, strong password policies, multi-factor authentication, and secure credential management significantly reduce vulnerability to attack. Employee education is equally important, as informed users are better equipped to recognize phishing attempts, suspicious links, and social-engineering tactics. Regular training programs and clearly defined security policies strengthen organizational resilience and reduce the likelihood of incidents caused by human error.

Future developments in device security are expected to rely increasingly on artificial intelligence, behavioral analytics, and advanced authentication technologies. AI-based security systems offer opportunities for real-time threat detection and automated response[28], while next-generation biometric solutions promise more adaptive and secure user verification. At the same time, security protocols are becoming more user-friendly, encouraging wider adoption without compromising protection.

In conclusion, the security of mobile and stationary devices remains a critical element of cybersecurity. Protection against malware, unauthorized access, data breaches, and physical loss requires a multilayered approach that combines technological safeguards, organizational measures, and user awareness. Through continuous modernization, effective security practices, and ongoing education, organizations and individuals can strengthen resilience against evolving cyber threats and maintain secure digital environments.

Summary

Today's information society faces an increasingly complex and dynamic cybersecurity landscape that requires a multifaceted approach. The evolving nature of cyberthreats, characterized by advanced malware, AI-based attacks, and zero-day exploits, requires a robust and adaptive cybersecurity infrastructure equipped with advanced technologies such as behavioral analytics and AI-based defenses. Equally important is the establishment of comprehensive legal and regulatory frameworks at the national and international levels to coordinate actions, enforce standards, and effectively combat cybercrime.

However, technology and regulations alone are not sufficient without addressing the crucial human factor, as user behavior and awareness significantly impact overall security. Increasing cybersecurity competencies through ongoing education, training, and fostering a security-first mindset among users is crucial to mitigating human vulnerabilities, such as weak passwords and susceptibility to social engineering. Together, these strategies create a resilient shield capable of defending against the myriad cyberthreats that threaten social stability, economic prosperity, and individual privacy. As technology continues to

[28] N. Katiyar, AI and Cyber-Security: Enhancing threat detection and response with machine learning, „Educational Administration Theory and Practice journal” 2024, vol. 30(4), p. 6276.

advance and cyberspace evolves, continuous adaptation, collaboration, and awareness remain crucial to securing our digital future.

Bibliography

Armoogum S. et al., A Comprehensive Review of Cyber Hygiene Practices in the Workplace for Enhanced Digital Security, „JOIV International Journal on Informatics Visualization" 2025, vol. 9(1).

Blessing G. et al., The Emerging Threat of Ai-driven Cyber Attacks: A Review, „Applied Artificial Intelligence" 2022, vol. 36(1).

Diana L., Dini P., Paolini D., Overview on Intrusion Detection Systems for Computers Networking Security, „Computers" 2025, vol. 14(3).

Duraisamy B., Chakrabarti A., Midhunchakkaravarthy D., Smart Devices Threats, Vulnerabilities and Malware Detection Approaches: A Survey, „European Journal of Engineering and Technology Research" 2018, vol. 3(2).

Faíscas D., (In)Security in Wi-Fi networks: a systematic review, „ARIS2 - Advanced Research on Information Systems Security" 2022, vol. 2(2).

Folorunso A., Security compliance and its implication for cybersecurity, „World Journal of Advanced Research and Reviews" 2024, vol. 24(01).

Hariyani D. et al., A literature review on transformative impacts of blockchain technology on manufacturing management and industrial engineering practices, „Green Technologies and Sustainability" 2025, vol. 3(3).

Hariyani D., Hariyani P., Mishra S., The role of leadership in sustainable digital transformation of the organization, „Sustainable Futures" 2025, vol. 10.

Jiang J., Ross J., Bai G., Ransomware Attacks and Data Breaches in US Health Care Systems, „JAMA Network Open" 2025 8(5).

Jyothi K., Reddy I., Study on Virtual Private Network (VPN), VPN's Protocols and Security „International Journal of Scientific Research in Computer Science, Engineering and Information Technology" 2018, vol. 3(5).

Katiyar N., AI and Cyber-Security: Enhancing threat detection and response with machine learning, „Educational Administration Theory and Practice journal" 2024, vol. 30(4).

Kumar S. et al., Secure data encryption key scenario for protecting private data security and privacy, „Journal of Discrete Mathematical Sciences and Cryptography" 2024, vol. 27(2).

Kvyetnyy R. et al., Critical cybersecurity aspects for improving enterprise digital infrastructure protection, „IAPGOŚ" 2025, vol. 1.

Mbah G., Data Privacy and the Right to be Forgotten, „World Journal of Advanced Research and Reviews" 2022, vol. 16(02).

Shomope A., Adeniyi A., Enhancing Digital Security: A Comprehensive Review of Password Management Practices and Tools, „International Journal Of Mathematics And Computer Research" 2025, vol. 13(02).

Tamrakar A., Patra B., Cybersecurity threats and countermeasures: a review, „Turkish Journal of Computer and Mathematics Education (TURCOMAT)" 2018, vol. 9(3).

Tanti R., Study of Phishing Attack and their Prevention Techniques, „Interantional Journal Of Scientific Research In Engineering And Management" 2024, vol. 8(10).

Ullah I., Boreli R., Kanhere S., Privacy in targeted advertising on mobile devices: a survey, „International Journal of Information Security" 2022, vol. 22(12).

Williamson J., Curran K., Best Practice in Multi-factor Authentication, „Semiconductor Science and Information Devices" 2021, vol. 3(1).

Zannettou S. et al., Understanding Web Archiving Services and Their (Mis)Use on Social Media, „Proceedings of the International AAAI Conference on Web and Social Media" 2018, vol. 12(1).

Zhang X., Data breach: analysis, countermeasures and challenges, „International Journal of Information and Computer Security" 2022, no. 19(3/4).

Rane S., The impact of social media on self-presentation and perception: navigating identity, communication, and connectivity in the digital age, https://www. researchgate. net/lab/Smita-Rane-Lab [access 30.12.2025].

Sharma I., Aggarwal A., Digital Footprints and the Battle for Data Sovereignty: Digital Privacy, Security, and Ownership, Driving Decentralization and Disruption With Digital Technologies, DOI: 10.4018/979-8-3693-3253-5.ch005.

Singh D., Parekh D., Khandelwal T., The WannaCry Attack: How it Worked and What We Learned, DOI: 10.13140/ RG.2.2.19481.74084 [access 05.01.2026].

Thomas J., A Case Study Analysis of the Equifax Data Breach 1 A Case Study Analysis of the Equifax Data Breach, 2019, DOI: 10.13140/RG.2.2. 16468.76161 [access 04.01.2026].