http://doi.org/10.35784/iapgos.7498 *received: 28.03.2025 | revised: 30.07.2025 | accepted: 25.08.2025 | available online: 30.09.2025*

ETHICAL SIMULATION OF A PHISHING ATTACK

Justyna Kęczkowska, Karol Wykrota, Mirosław Płaza
Kielce University of Technology, Kielce, Poland

Abstract. *This article presents an ethical simulation of a phishing attack as a research method for analysing users' susceptibility to such threats. The study involved conducting an experiment in which emails mimicking authentic messages from popular services such as Google, Spotify, and InPost were sent. A total of 50 participants were involved in the experiment, divided into five age groups, allowing for an assessment of the impact of age on phishing attack susceptibility. The aim of the study was to determine the effectiveness of various social engineering techniques and to analyse users' reactions to the fraudulent messages. The experiment utilized dedicated, proprietary software that enabled monitoring of recipient activity, including reading messages, opening URLs, and filling out forms. The results showed that most users opened the phishing emails; however, only a small percentage took further actions that could potentially lead to data disclosure. The analysis of the results confirmed the crucial role of educational factors and user awareness in mitigating the effectiveness of phishing attacks. A particularly significant aspect was users' prior experience with similar attacks and their active participation in informational campaigns, which significantly reduced their susceptibility to manipulation. In conclusion, recommendations were formulated emphasizing the need for systematic training campaigns and the implementation of advanced email filtering systems, which are crucial in counteracting the threats discussed in this study.*

Keywords: phishing, cyberattack, computer hacking, cybersecurity

ETYCZNA SYMULACJA ATAKU PHISHINGOWEGO

Streszczenie. *W artykule przedstawiono etyczną symulację ataku phishingowego jako metodę badawczą służącą do analizy podatności użytkowników na tego typu zagrożenia. Badanie obejmowało przeprowadzenie eksperymentu, w ramach którego rozesłano wiadomości e-mail imitujące autentyczne komunikaty otrzymywane od popularnych serwisów, takich jak: Google, Spotify oraz InPost. W eksperymencie wzięło udział 50 uczestników podzielonych na pięć grup wiekowych, co umożliwiło ocenę wpływu wieku na podatność ataków phishingowych. Celem badania było określenie skuteczności różnych technik inżynierii społecznej oraz analiza reakcji użytkowników na przesyłane fałszywe wiadomości. W eksperymencie zastosowano dedykowane, autorskie oprogramowanie umożliwiające monitorowanie aktywności odbiorców, w tym w zakresie: odczytywania wiadomości, otwierania adresów URL oraz wypełniania formularzy. Wyniki badania wykazały, że większość użytkowników otworzyła wiadomości phishingowe, jednak tylko niewielki odsetek podjął dalsze działania prowadzące do potencjalnego ujawnienia danych. Przeprowadzona analiza wyników potwierdziła kluczową rolę czynników edukacyjnych oraz świadomości użytkowników dotyczących potencjalnych zagrożeń w ograniczaniu efektywności ataków phishingowych. Szczególnie istotnym aspektem okazało się wcześniejsze doświadczenie użytkowników z podobnymi atakami oraz aktywny udział w kampaniach informacyjnych, co znacząco zredukowało ich podatność na manipulacje. W konkluzji sformułowano rekomendacje dotyczące konieczności systematycznego prowadzenia kampanii szkoleniowych oraz implementacji zaawansowanych systemów filtrowania wiadomości elektronicznych, mających kluczowe znaczenie w przeciwdziałaniu opisywanym w pracy zagrożeniom.*

Słowa kluczowe: phishing, cyberatak, hakowanie komputerów, cyberbezpieczeństwo

Introduction

For a long time now, issues related to online privacy have affected not only the commercial sector but also private users [5, 9, 15, 20, 27, 31]. Cybercriminals often exploit low public awareness to obtain sensitive data, which is later used for criminal purposes. Analysing potential threats in cyberspace reveals a significant increase in dangers associated with social engineering attacks. These attacks frequently rely on personal relationships and interpersonal trust, evoking positive or negative emotions [1, 4, 6, 17, 22, 28]. Their effectiveness is based on interactions with end-users of a system, meaning that even the most advanced technological solutions cannot always protect users from social engineering attacks. In such cases, the only means of protection is raising user awareness and providing extensive education [14, 18, 21, 26, 32].

One of the most widespread and dangerous forms of cyberattacks using social engineering techniques to steal confidential information is phishing [7, 10, 13, 33]. A typical phishing attack begins with sending the target a fraudulent message that appears authentic. This message often contains a link to a fake website that impersonates a legitimate institution. By entering their credentials, the recipient unknowingly hands them over to the attacker [11, 25, 30]. Phishing attacks can exploit various communication channels, including traditional email messages, SMS messages (smishing), phone calls conducted by telecom operators or call/contact centre systems (vishing), as well as IoT-based solutions [3, 8, 16, 19, 23, 24, 29]. Advanced spear phishing attacks targeting specific individuals or organizations are also increasingly observed [12]. According to the 2024 Verizon Data Breach Investigations Report [38], phishing accounted for approximately 20% of all hacking attacks conducted in 2023. This highlights the growing scale of the problem and the need for continuous improvement of defence mechanisms against such threats [2]. The escalating challenges in cybersecurity motivated the authors to conduct research on users' susceptibility to phishing-based attacks.

This article presents an ethical simulation of phishing attacks with varying themes and different data extraction mechanisms. The aim of the conducted experiments was to raise awareness among private users about the threats posed by phishing. The research findings presented in this study allowed for an assessment of the effectiveness of potential attacks using social engineering techniques. Additionally, the simulations enabled an evaluation of the security mechanisms implemented in popular online services and helped identify the most vulnerable areas. The experiments were educational in nature, and the obtained results may serve as a foundation for further research and the development of tools to support testing and training users in recognizing phishing attacks.

1. Research methodology

The research methodology for conducting the ethical simulation of a phishing attack described in this study involved the following stages:

- collecting necessary data using publicly available sources, defining the topics and content for the fabricated messages,
- developing dedicated software to automate phishing attack processes,
- conducting the ethical phishing attack simulation under controlled real-world conditions according to the designed scenario.

1.1. Data preparation

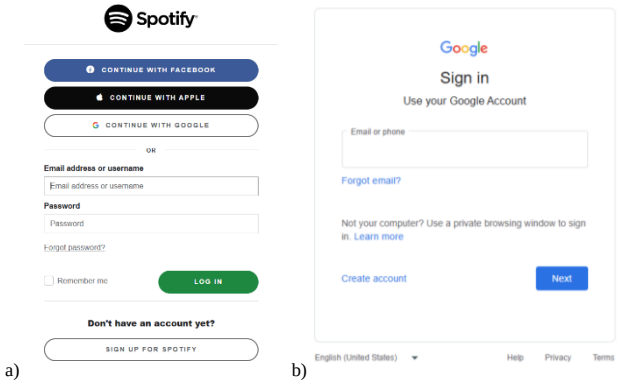
For the study, three message topics were selected, each targeting users of three different services: Spotify, Google and InPost. Spotify users received a false notification about an alleged subscription loss. Google account holders were sent

a fake security alert. InPost users received messages regarding supposed delivery issues. The topics and content of the messages were designed to capture recipients' interest and prompt a quick reaction. Additionally, the messages were crafted to closely resemble authentic communications sent by the respective organizations. Messages appearing to come from Spotify and Google contained a hyperlink leading to a fraudulent website (mock interfaces are shown in figure 1), while InPost users received a malicious attachment. Table 1 presents the prepared data sets.

Table 1. Overview of fraudulent e-mails

Recipient platform	Subject and content of the message	Type of attachment
Spotify	Subject: *You no longer have access to Premium services.* Content: *User xxx (where xxx is a name generated based on the recipient's email address) no longer has access to the Premium Family plan. You are now using the free plan. Want to learn more? Click the button below.*	Link to the fraudulent website
Google	Subject: *New log-in from a Windows device* Content: *We have detected a new login to your Google account from a Windows device. If this was you, no action is needed. If not, we can help you secure your account. Check your activity by clicking the link below!*	Link to the fraudulent website
Inpost	Subject: It has arrived! Content: *It's your move! Your package is in the Parcel Locker. The attachment contains shipment details. If you don't pick up your package within the designated time, it will be returned to the sender – and we wouldn't want that!*	Malicious attachment

The message content was designed to incorporate various social engineering techniques to prompt recipients into reckless actions. A key strategy was leveraging well-known brands to establish a sense of trust among recipients. Additionally, the messages aimed to create a sense of urgency or threat – for example, by informing users of lost access to paid services or issuing security alerts. The content also referenced everyday user experiences, such as receiving packages, and strategically aligned with periods of high shopping activity to make the message appear more credible.



a) b)

Fig. 1. Prepared Web Pages Resembling: a) Spotify, b) Google

Fig. 2. Message informing about ethical simulation

Figure 1 presents the prepared web overlays, whose informational content was recreated using HTTrack software. The visible forms were modified to allow the server to register when a user submitted the form. This was achieved by embedding a PHP script into the document structure. Due to the nature of the experiment, the data entered by users was not monitored or archived on the server side. Full anonymity was ensured by not collecting any personal data that would enable the identification of the participants in the experiment. The data processing was in line with the applicable data protection laws, including Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR). For ethical reasons and in line with the principle of risk minimization, participants were informed about the nature of the experiment immediately after they took any action. The user was then informed via a pop-up banner that they were participating in an ethical phishing attack simulation experiment (the appearance of the message is shown in figure 2). Each person who attempted to share their data was given educational guidance on how to avoid such attempts to obtain information.

1.2. Software

To conduct the attack, a proprietary software environment was developed, enabling the fully automated sending of the prepared messages. The core functionalities of the developed system include the ability to define all parameters of the sent messages (recipient address, sender address, sender name, subject, content) and the option to track information regarding the progress of the attack. The system's flowchart, illustrating its operation, is presented in figure 3.

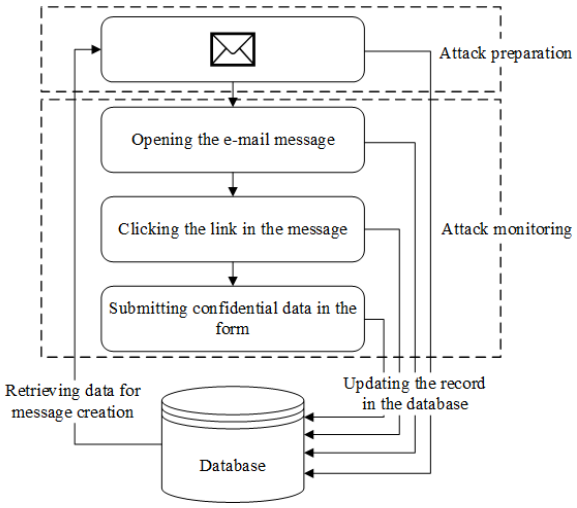


Fig. 3. Block diagram of the developed system

The environment was developed using the PHP language [36], utilizing the SQLite 3 module [37] embedded in the language interpreter. This module was used to store information about the sent email messages. In the initial phase, the parameters of each message must be specified. To do this, relevant records are fetched from the database, containing information such as: a) email addresses of message recipients, b) sender's email address (the address displayed in the message header), c) sender's name (which appears in the email client message list), d) the subject and content of the generated message. In the next phase of the system's operation, the message content is sent to the intended recipients. It was assumed that the content would be generated as a text/HTML field, enabling the use of graphical elements. This allowed the inclusion of a 1-pixel graphic element in the content, which communicated with the server through GET requests. The attack process, representing the next phase of the system, was monitored using the function md5(rand()), generating a unique identifier for each message. This identifier helped track the actions of individual recipients. For the web

pages, the following actions were monitored: a) the recipient opening the message, b) the user activating the provided link, c) the user submitting the completed form. For the attachment, the following actions were monitored: a) the recipient opening the message, b) the recipient opening the attachment.

The developed IT environment offers scalability, allowing experiments to be extended to a larger group of users by appropriately configuring the recipient database and adjusting message sending parameters. The system can be expanded with additional modules that monitor other types of user interactions, such as time spent on fake websites. The modular architecture of the solution allows for the addition of new attack scenarios and integration with external security systems in the future.

1.3. Experiment

Based on the prepared automated IT environment and the generated messages, a dedicated scenario for the simulated attack was developed, consisting of four steps. In the first step, the target group of recipients was selected. Participants for the experiment were chosen from the close social environment of the study's authors, allowing for controlled social context within the experiment. The participants were not informed about the true nature of the received messages, ensuring authentic reactions to the simulated phishing attacks. The research sample included 50 individuals divided into five age groups as follows: <18, (18–26>, (27–36>, (37–46>, >46. This method of selecting respondents ensured a high level of reliability in the data analysis process. It also allowed for an assessment of the impact of age on susceptibility to phishing attacks. The age distribution of the selected target group, along with the sample sizes, is presented in figure 4.

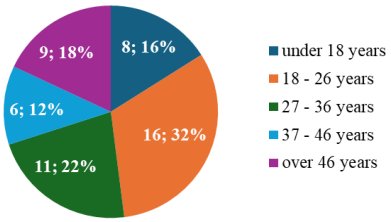


Fig. 4. Percentage distribution of age groups among the surveyed respondents

In the second step, to enhance the effectiveness of the experiment, an OSINT analysis was conducted, allowing the phishing messages to be tailored to the actual interests of the participants. As a result, the messages referenced services that the recipients genuinely used, increasing the likelihood of interaction. The typical user interactions with the platforms mentioned in Section 1.1 were analysed. This was to gain insights that would improve the preparation of the simulated attack.

The next stage of the experiment involved executing the attack itself. Messages targeting Spotify and InPost users were sent to recipients with email accounts hosted on the following mail servers: gmail.com, wp.pl, o2.pl, op.pl, interia.pl, onet.pl, and outlook.com. Meanwhile, the security alert messages were directed exclusively to users with email addresses in the gmail.com domain. The simulated attack was carried out using the developed software, which is described in detail in Section 1.2. The attack monitoring process was conducted as follows:

- when a recipient opened the email, a response was sent to the server in the form of an identifier. Based on this identifier, the server determined the date and time of the user's action.
- from that moment, the system entered a standby mode, waiting for either the activation of the embedded link or the opening of the attachment. If the user activated the link or opened the PDF attachment, the action was recorded and sent to the server. Based on this data, the server determined the exact date and time of the action. Additionally, InPost users received a follow-up email informing them that they had unknowingly participated in a simulated phishing attack.
- for users who filled out and submitted the form (applicable to messages addressed to Spotify and Google users), a pop-up notification was displayed, informing them about their participation in the simulated phishing attack. To maintain ethical and legal compliance (e.g., GDPR regulations), any data entered by users was neither stored nor collected.

The final step involved analysing the gathered data and assessing the effectiveness of the study, as described in Section 2.

2. Results and discussion

The use of an identifier that allowed tracking the various stages of the simulated phishing attack enabled monitoring of the delivery path of the sent messages. For emails falsely attributed to Google, messages were sent to 30 participants in the simulation. The remaining messages (InPost, Spotify) were sent to all 50 participants (Fig. 5). Some messages (18%) that appeared to come from InPost or Spotify did not reach the recipients (10%) or were blocked by the recipient's email security mechanisms and marked as spam (8%). On Microsoft servers (responsible for outlook.com), the emails were filtered into the spam folder. Meanwhile, messages sent to onet.pl domains were completely blocked. Figure 5 presents the quantitative distribution of delivered messages: Green indicates emails that successfully reached the recipient's inbox. Blue represents messages that were filtered into spam folders. Red marks emails blocked by security mechanisms.

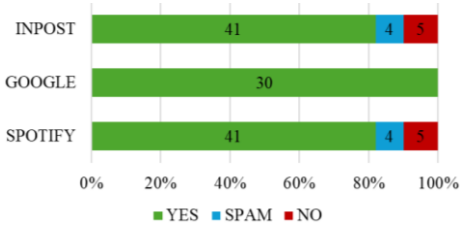


Fig. 5. Effectiveness of the message delivery process, where: YES – emails that successfully reached recipients' inboxes; SPAM – emails that were filtered into the spam folder; NO – emails that were blocked

It follows that mechanisms for controlling delivered correspondence also play a role in security. Some of the messages sent were blocked by email security systems – spam filters, DMARC rules, and mail server-level blocks. This confirms that system solutions can support users in effectively protecting themselves against phishing, but ultimately, user awareness in this area is crucial to ensuring security. The majority of messages that reached the inbox were opened by recipients, as shown in table 2.

Table 2. Actions taken by users

User action		Platform		
		Spotify	Google	Inpost
Ignored		37%	10%	44%
Message opened		63%	90%	56%
and	link / attachment opened	35%	15%	35%
	Form filled out	8%	4%	n/a

Most participants in the simulation only opened the attached form or clicked on the provided link. Only a few of them actually filled out the form. For emails allegedly from InPost, none of the recipients provided the requested information. This could be due to the fact that InPost customers have been frequently targeted by cybercriminals in the past, receiving fraudulent emails and SMS messages. Reports of the first phishing attacks on InPost customers date back to 2020 [35]. Cybercriminals typically increase their activity during sales periods or holiday shopping seasons, hoping that the higher volume of package orders will cause customers to lower their guard and be more likely to provide

their details. Since these attacks have been repeated for several years, InPost has implemented awareness campaigns to educate its customers about phishing threats [34]. The lack of user interaction with these messages may confirm the effectiveness of educational initiatives as a strong protective measure against phishing.

Recipients of the fraudulent emails were informed after the mailing campaign had concluded that they had participated in an ethical hacking simulation and were asked to complete a survey consisting of seven questions. These questions focused on respondents' awareness of phishing and their past experiences with potentially dangerous emails. The survey specifically analysed user behaviour when receiving and opening messages, including how they verified the sender and inspected links within the content. An essential part of the survey aimed to assess participants' level of distrust toward received emails and the links contained within them. The survey also included a demographic section where users provided their age range. Only responses from participants who were involved in the simulated phishing attack were analysed.

60% of respondents indicated that they understand what phishing is. The highest awareness was observed among individuals under 18 years old (88%), likely due to their daily engagement in the digital world and access to current education on internet security. At the same time, 40% of respondents did not recognize the scale of the phishing problem, making them potentially easy targets for attacks. Additionally, 48% of participants reported having received emails in the past that contained links to fraudulent websites. This finding highlights the widespread nature of the issue while also indicating a low level of awareness among recipients, as many are unable to identify phishing emails. Almost all users confirmed that they always check the sender's email address, which theoretically could contribute to their level of security. Figure 6 presents the percentage of survey participants who verified the sender's email address, broken down by age groups. Green represents individuals who declared that they verify the sender's email address, while red represents those who do not.

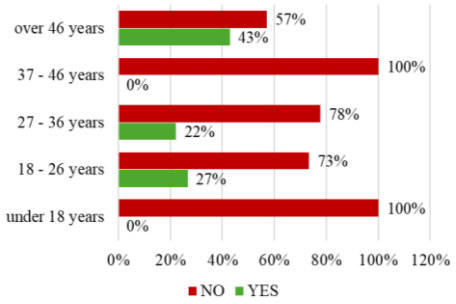


Fig. 6. Verification of the sender's email address in different age groups, where: YES – address was verified, NO – address was not verified

For most respondents, emails and websites accessed through embedded links appeared somewhat suspicious (24% and 20% of respondents, respectively). The discrepancies in content evaluation confirm that, despite a limited level of trust, users may lack the knowledge or tools necessary to effectively recognize sophisticated fraud attempts.

The conducted simulation demonstrated that users react to phishing attacks to varying degrees, and their susceptibility depends on the content of the message and the applied social engineering techniques. The results confirm that user education and appropriate protective mechanisms play a crucial role in minimising the risk of such threats. Additionally, it was observed that previous experiences with phishing attacks may influence users' caution and their responses to suspicious messages.

3. Conclusion

Based on the conducted simulation, it can be concluded that, regardless of the selected age group, knowledge about phishing is insufficient. This confirms the need for educational campaigns aimed at all users. A significant challenge for system administrators is to develop effective tools for educating end users. The proposed solution can serve as a foundation for conducting ethical simulations of attacks among internet users. This could be the first step in training users to recognize phishing attacks.

To increase awareness and improve security, it is essential to implement regular training sessions and workshops for employees, which will help them in recognizing and responding to phishing attacks. It is also worth implementing email filtering and analysis systems that automatically detect and block phishing attempts, which significantly reduces risk. Conducting phishing attack simulations can help test employee vigilance and identify areas that need improvement. Additionally, establishing clear procedures for reporting suspicious emails will encourage employees to actively participate in protecting the organization.

In the context of further work on the development of the described system, it is planned to conduct research with a larger number of participants, as well as to expand the existing solution into a dedicated application supporting training processes in the field of protection against social engineering attacks.

References

[1] Aiden M. K., et al.: Social Engineering Attacks: Detection and Prevention. Shrivastava G., et al. (eds): Emerging Threats and Countermeasures in Cybersecurity. Scrivener Publishing LLC 2025, 349–387.
[2] Akyeşilmen N., Alhosban A.: Non-Technical Cyber-Attacks and International Cybersecurity: The Case of Social Engineering. Gaziantep University Journal of Social Sciences 23(1), 2024, 342–360.
[3] Alkhalil Z., et al.: Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science 3, 2021, 563060.
[4] Alshammari S. S., Soh B., Li A.: Understanding Social Engineering Victimisation on Social Networking Sites: A Comprehensive Review of Factors Influencing User Susceptibility to Cyber-Attacks. Information 16(2), 2025, 153.
[5] Admass W. S., Munaye Y. Y., Diro A. A.: Cyber security: State of the art, challenges and future directions. Cyber Security and Applications 2, 2024, 100031.
[6] Choi Y. B.: Social Engineering Cyber Threats. Journal of Global Awareness 4(2), 2023, 8.
[7] Chanti S., Chithralekha T.: A literature review on classification of phishing attacks. International Journal of Advanced Technology and Engineering Exploration 9(89), 2022, 446–476.
[8] Chanti S., Chithralekha T.: A literature review on classification of phishing attacks. International Journal of Advanced Technology and Engineering Exploration 9(89), 2022, 446–476
[9] Lee N.: Cyberattacks, Prevention, and Countermeasures. Lee N. (ed.): Counterterrorism and Cybersecurity: Total Information Awareness. Springer International Publishing, Cham 2024, 295–342.
[10] Gallo L., et al.: The human factor in phishing: Collecting and analysing user behavior when reading emails. Computers & Security 139, 2024, 103671.
[11] Goenka R., Chawla M., Tiwari N.: A comprehensive survey of phishing: Mediums, intended targets, attack and defence techniques and a novel taxonomy. International Journal of Information Security 23(2), 2024, 819–848.
[12] Ghazi-Tehrani A. K., Pontell H. N.: Phishing evolves: Analyzing the enduring cybercrime. Victims & Offenders 16(3), 2022, 316–342 [https://doi.org/10.1080/15564886.2020.1829224].
[13] Gupta S., et al.: A Comprehensive Analysis of Social Engineering Attacks: From Phishing to Prevention-Tools, Techniques and Strategies. Second International Conference on Intelligent Cyber Physical Systems and Internet of Things – ICoICI, 2024, 1–8.
[14] Hakimi M., Quchi M. M., Fazil A. W.: Human factors in cybersecurity: an in depth analysis of user centric studies. Jurnal Ilmiah Multidisiplin Indonesia – JIM-ID 3(01), 2024, 20–33.
[15] Jeon G.H., et al.: IWTW: A Framework for IoWT Cyber Threat Analysis. CMES-Computer Modeling in Engineering & Sciences 141(2), 2024, 1575–1622 [https://doi.org/10.32604/cmes.2024.053465].
[16] Jain A. K., Gupta B. B.: A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems 16(4), 2022, 527–565.
[17] Kamruzzaman A., et al.: Social engineering incidents and preventions. IEEE 13th Annual Computing and Communication Workshop and Conference – CCWC, 2023, 0494–0498.

[18] Kont K. R.: Libraries and cyber security: the importance of the human factor in preventing cyber attacks. Library Hi Tech News 41(1), 2024, 11–15.
[19] Kumar S., Gouda S.: A Comprehensive Study of Phishing Attacks and Their Countermeasures. International Journal of Research and Analytical Reviews 10, 2023, 25–31.
[20] Mallick M. A. I., Nath R.: Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News 190(1), 2024, 1–69.
[21] Oladipo J. O., et al.: Human factors in cybersecurity: Navigating the fintech landscape. International Journal of Science and Research Archive 11(1), 2024, 1959–1967.
[22] Parsaei A.: Awareness and social engineering-based cyberattacks. International Journal of Reliability, Risk and Safety: Theory and Application 7(1), 2024, 31–36.
[23] Płaza M., et al.: Machine Learning Algorithms for Detection and Classifications of Emotions in Contact Center Applications. Sensors 22(14), 2022, 5311 [https://doi.org/10.3390/s22145311].
[24] Płaza M., Belka R., Szcześniak Z.: Towards a different world – on the potential of the internet of everything. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska – IAPGOS 2, 2019, 8–11.
[25] Putra F. P. E., et al.: Analysis of phishing attack trends, impacts and prevention methods: literature study. Brilliance: Research of Artificial Intelligence 4(1), 2024, 413–421.
[26] Scherb C., et al.: A cyber attack simulation for teaching cybersecurity. EpiC Series in Computing 93, 2023, 129–140.
[27] Shukla R. K., Tiwari A. K.: Security analysis of cyber-crime. Shukla R. K., et al. (eds.): The Ethical Frontier of AI and Data Analysis. IGI Global, 2024, 257–271
[28] Siddiqi M. A., Pak W., Siddiqi M. A.: A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences 12(12), 2022, 6042.
[29] Sonowal G.: Types of Phishing. Sonowal G.: Phishing and Communication Channels: A Guide to Identifying and Mitigating Phishing Attacks, 2022, 25–50.
[30] Tian C., et al.: The influence of affective processing on phishing susceptibility. European Journal of Information Systems 34(3), 2024, 1–15.
[31] Yi Z., Chen X.: Personal Privacy Protection Problems in the Digital Age. arXiv preprint arXiv:2211.09591, 2022.
[32] Zhang-Kennedy L., Chiasson S.: A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys – CSUR 54(1), 2021, 1–39.
[33] Zangana H. M., et al.: Cybernetic Deception: Unraveling the Layers of Email Phishing Threats. International Journal of Research and Applied Technology – INJURATECH 4(1), 2024, 35–47.
[34] InPost – Plaga ataków phishingowych – chroń swoje dane! 2025 [https://inpost.pl/aktualnosci-plaga-atakow-phishingowych-chron-swoje-dane].
[35] Niebezpiecznik – Uwaga na SMS-y podszywające się pod Inpost. 2025 [https://niebezpiecznik.pl/post/uwaga-na-sms-y-podszywajace-sie-pod-inpost/].
[36] The PHP Documentation Group – PHP Manual. 2025 [https://www.php.net/manual/en/].
[37] The PHP Documentation Group – SQLite3. 2025 [https://www.php.net/manual/en/book.sqlite3.php].
[38] Verizon Business – 2024 Data Breach Investigations Report. 2024 [https://www.verizon.com/business/resources/reports/dbir/].

Ph.D. Justyna Kęczkowska
e-mail: j.keczkowska@tu.kielce.pl

Since 2002, she has been a member of the academic staff at the Kielce University of Technology. She obtained the title of Doctor of Technical Sciences in 2011 in Military University of Technology in Warsaw. She has participated in research and development work under EU-funded projects. She is the author of more than 50 scientific publications and co-author of two patents. Her scientific interests include new nanomaterials for electronics, artificial intelligence systems and cyber security with a focus on social engineering attacks.

https://orcid.org/0000-0002-2309-3065

M.Sc. Karol Wykrota
e-mail: k.wykrota@tu.kielce.pl

He holds an M.Sc. in Computer Science with a specialization in cybersecurity, which he earned from Kielce University of Technology in 2024. Currently, he is a faculty member in the Faculty of Electrical Engineering, Automatic Control and Computer Science. His interest is to research in the fields of network and system security.

https://orcid.org/0009-0000-4179-6779

Ph.D. Mirosław Płaza
e-mail: m.plaza@tu.kielce.pl

Since 2002, he has been a member of the academic staff at the Kielce University of Technology, where he obtained the title of Doctor of Technical Sciences in 2015. He is the head of ICT&IoT CyberLAB and the head and instructor of Cisco Networking Academy. He has conducted numerous R&D studies for EU-financed projects. He is the author of one monograph, and over 50 scientific publications. He is a winner of the international European Kangaroo Mathematics Contest, where he won the main prize.

https://orcid.org/0000-0001-9728-3630