SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 177

ANALYSIS OF THE LEVEL OF AWARENESS AMONG THE ACADEMIC COMMUNITY IN THE FIELD OF CYBERSECURITY

Anna KILJAN[1*], Adrian KAPCZYŃSKI[2]

[1] Silesian University of Technology, Faculty of Mechanical Engineering; anna.kiljan@polsl.pl, ORCID: 0000-0002-1560-3408
[2] Silesian University of Technology, Faculty of Applied Mathematics; adrian.kapczynski@polsl.pl, ORCID: 0000-0002-9299-1467
* Correspondence author

Purpose: The purpose of the work was to discuss various forms of social engineering and to conduct a survey among the academic community in the field of cybersecurity.
Design/methodology/approach: Survey was conducted by google forms.
Findings: The paper discusses the issue of social engineering and its types, such as: phishing, pharming, vishing, whaling, skimming and rubber ducky devices. Subsequently, "good practices", i.e. recommendations to be used in order to increase security against a cyberattack, were discussed. In the research part, a survey was conducted among the academic community. 111 respondents took part in the survey. The answers were analyzed and conclusions were drawn. Research among the academic community on cybersecurity awareness has been conducted for the first time. The results show the level of awareness and demand for cybersecurity training.
Social implications: The survey was aimed at examining the awareness of the academic community in the field of cybersecurity. Based on the responses, it can be concluded that the demand for training in this area is high.

Keywords: cybersecurity; social engineering; awareness; cyberattack, academic community.

Category of the paper: Research paper.

1. Introduction

Over the years, the Internet has become not only a tool, but also a meeting place, work place, library, school, cinema, bank and many other facilities. Today, every generation, from children to seniors, uses the Internet. Opportunities offered by access to the network, unfortunately, also create threats, opportunities for fraudsters, a voice of hatred and facilitations

for all kinds of crimes (Dudzińska et al., 2020; Kiljan et al., 2022, Kowolik et al., 2021). That is why it is so important to make users aware of the dangers and threats.

The aim of the work was to discuss various forms of social engineering, to present "good practices" in order to increase the security of network use, and to conduct a survey among the academic community in the field of cybersecurity.

The survey was anonymous, and the respondents were students and employees of the Silesian University of Technology. The survey was aimed at examining the level of awareness in the field of cybersecurity and an indication of the need for training in this topic.

2. Social engineering

Due to the constant development of new hacking techniques, network security and protecting your computer becomes quite problematic. Unsecured hardware results in data loss through, for example, malware that can steal personal data after getting into the device, or malware that can damage or destroy files on the device (Lewandowska 2019; Garwol 2018; Furmanek 2012; Wojtkowiak et al., 2013).

Not only companies are attacked, but also individual network users. In order to protect against such events, you should block applications that seem suspicious, do not click on links of unknown origin, or do not connect unknown devices to the USB port, because dangerous software can be knowingly installed. You should also pay attention to the Internet network, whether it is properly secured and how it is made available. Another danger awaits users of social networking sites, providing information about themselves, posting photos without checking their privacy settings. It is important to encrypt data and important documents, and using the so-called virtual disk, i.e. the "cloud", files should be protected before being sent (Lewandowska, 2019; Czekaj, Stecko, 2016; Grubicka et al., 2019; Grubicka, Jopek, 2017).

The most popular threats in cyberspace include (Grzelak, Liedel, 2012; Walendzik, Wilkosz, 2018; Gronowicz, Woś, 2018; Jopek, Kinda, 2019; Noga et al., 2018; Kujawińska et al., 2021; Samociuk, 2023; Wawrowski et al., 2023):

- malware attacks (malware, viruses, worms, etc.);
- identity theft;
- theft (extortion), modification or destruction of data;
- blocking access to services (mail bombs, DoS and DDoS19);
- spam (unsolicited or unnecessary e-mails);
- social engineering attacks (e.g. phishing, i.e. phishing for confidential information by impersonating a trustworthy person or institution).

The elements of social engineering that are described in the next section are social engineering attacks. Social engineering is any attack that uses human psychology to perform certain actions or to transfer information in order to influence the target of the attack (Gray, 2023; Tomczyk, 2019). Online scammers sometimes work on their target for several months, gathering information about the victim, following social networks, analyzing behavior and trying to sense where they will hit in the search for information of interest to them. Research shows that the most common targets of social engineering attacks are people in managerial positions (Lizut et al., 2014; Kujawińska et al., 2021; Kowolik et al., 2021).

Social engineering can be an extremely effective tool for data mining. Internet fraud has been happening since the very beginning of the Internet. Cybercriminals come up with newer and newer techniques and tactics to deceive users. Only the vigilance of the user depends on recognizing the problem and avoiding fraud. If vigilance fails, the result is usually a financial loss (Cisowski et al., 2021).

3. Cybersecurity awareness survey

Recently, there has been an increasing interest in the topic of cyber security. Cybersecurity is also one of the pillars of Industry 4.0. However, due to the occurrence of cyberattacks and a lot of information in social media on this topic, it was found that conducting a cybersecurity awareness survey among the academic community of the Silesian University of Technology would be a good idea. 111 people responded to 307 questionnaires sent. The questionnaire was sent to employees and students of the Silesian University of Technology.

The survey consisted of 12 single and multiple choice questions. It was possible to answer "Other" than listed. The survey was conducted using a Google form. The survey was anonymous.

4. Summary of survey research

The results of the survey are presented below. Out of 307 respondents, 111 people answered.

111 people took part in the survey: 55 women, 52 men, while 4 people preferred not to disclose their gender (Fig. 1).

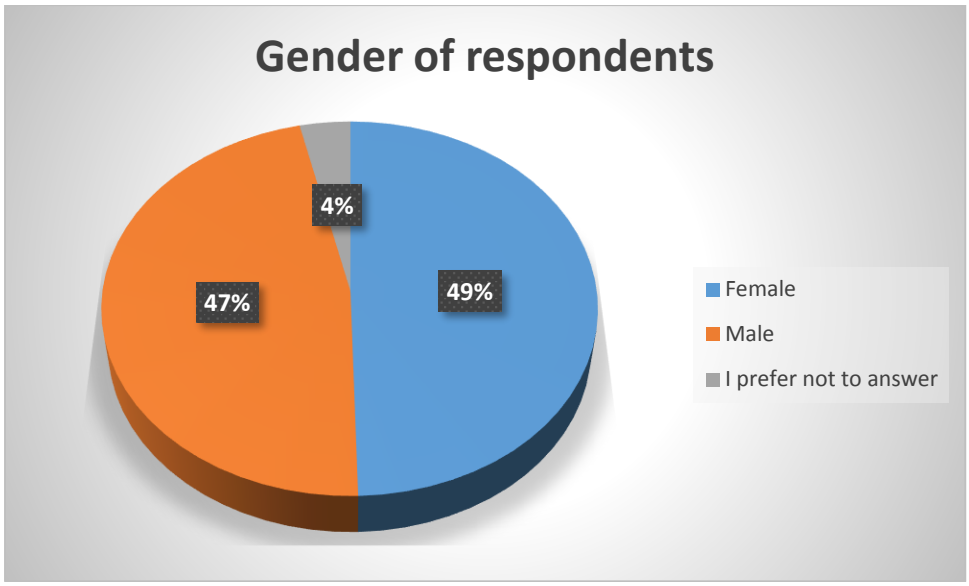

Figure 1. Gender of respondents.

Source: own elaboration.

Among the respondents (Fig. 2), the largest group of 70 people was aged 19-25, i.e. students. Subsequently, 15 people aged 37-47, 14 people aged 26-36, 11 people aged 48-58 and 1 person over 59 years of age.

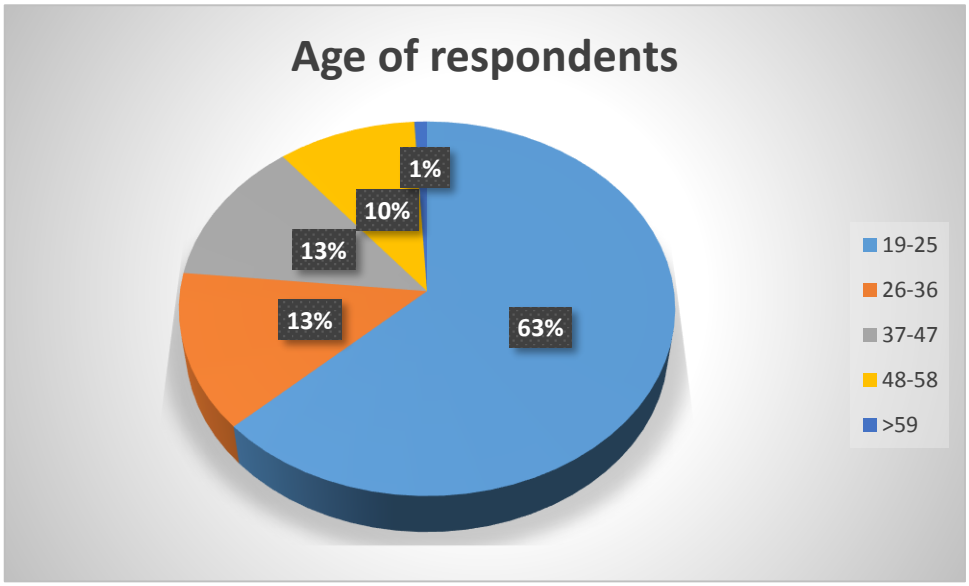

Figure 2. Age of renspondents.

Source: own elaboration.

The largest number of respondents (Fig. 3), as many as 50 people had secondary education. Another group, 33 people, higher education. 18 people had a PhD degree. 6 people had a habilitation, 2 people had higher education with post-graduate studies or MBA, and 2 people with a professorship.

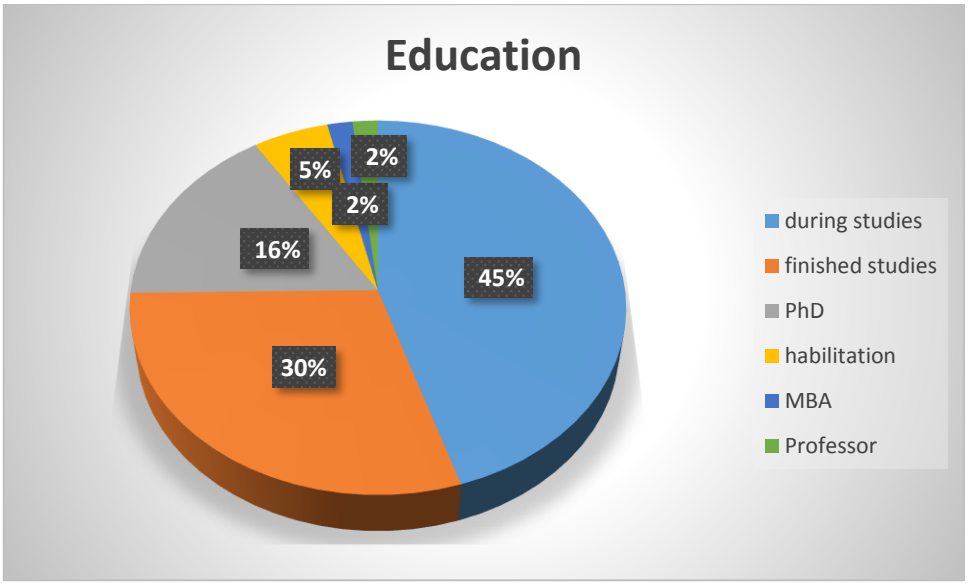

Figure 3. Education of respondents.

Source: own elaboration.

As many as 61 people declared the level of technical skills as medium. 47 people high level, i.e. advanced use of databases, programming and/or script execution. Only 3 people declared their level of technical skills as basic (Fig. 4).

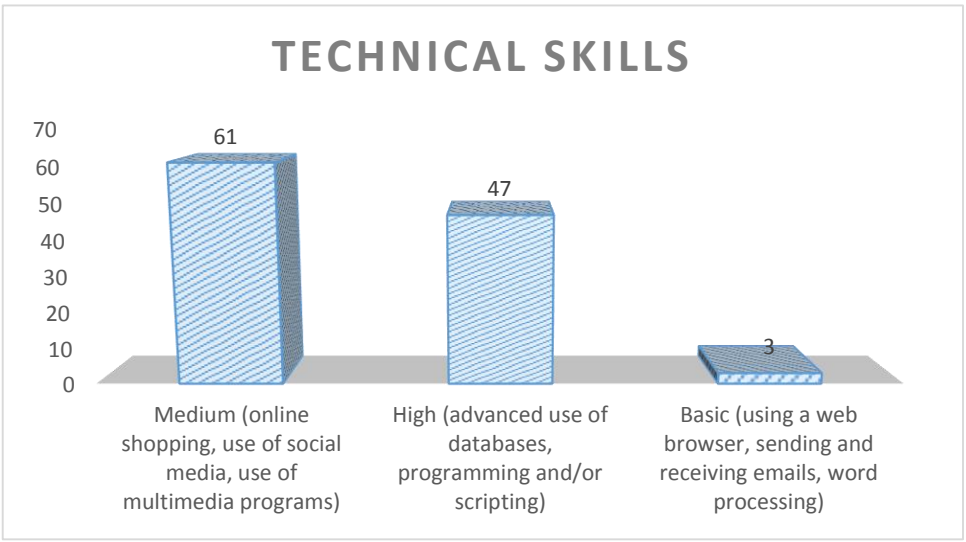

Figure 4. Technical skills of respondents.

Source: own elaboration.

Among the respondents (Fig. 5), the most well-known form of social engineering is phishing (more than half of the respondents). Unfortunately, as many as 45 people do not know any of the given forms. 29 people have heard of skimming. 16 people know what vishing is, 15 people know what rubber ducky is, 14 people know about pharming and whaling. Individuals also added: baiting, CEO, fraud, scareware, quid pro quo, bribing a company employee to install a suspicious program on the company's computer, ARP and XAMPP attacks.

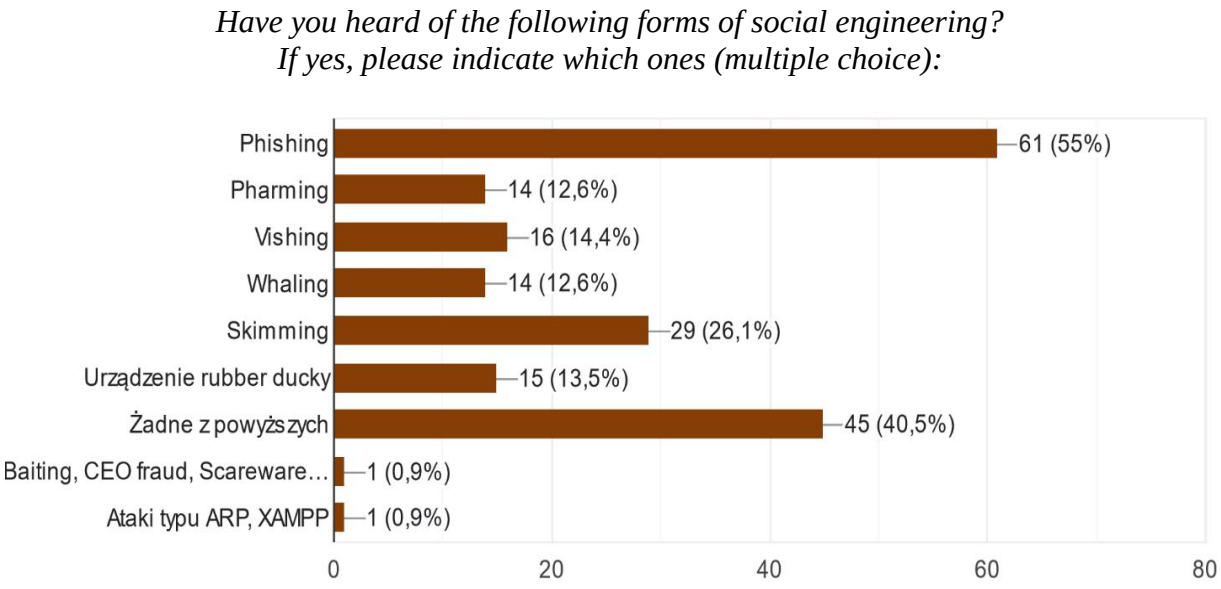

Figure 5. List of forms of social engineering.

Source: own elaboration.

101 people out of 111 respondents have had contact with a cyberattack, 10 people declare that they have not had such contact (Fig. 6).

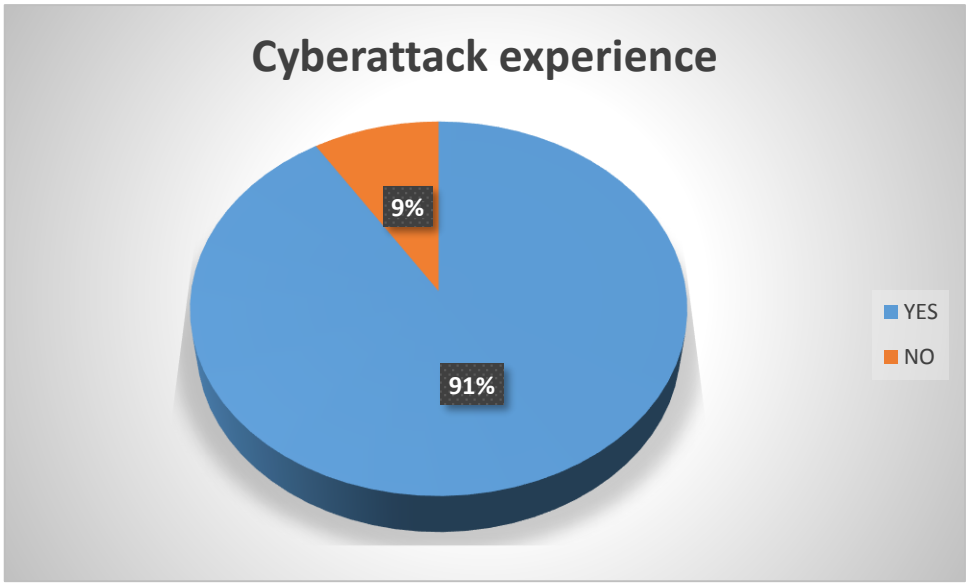

Figure 6. Cyberattack experience.

Source: own elaboration.

99 people declared that they had received a suspicious link sent by email or SMS in their lifetime. 79 received spam, which is quite a common and common form. 56 people were contacted via a fake profile on a social networking site. Almost 1/3 of people had telephone contact with a fraudster, for example, claiming to be a bank employee. 12 people had contact with installing dangerous software, also via USB devices. One person was not in contact with any attack.

Individuals mentioned:

- Scripts in pdf files, in MS Word editor files, in MS Excel spreadsheet files, e-mail attachments.
- Testing your own equipment to check security.
- Account hacking.
- Chatbots, intrusive ads with fees.
- Email messages testing the caution of plant employees.

109 people are aware (Fig. 7) that online activities are tracked to create an online profile and send advertisements. Only 2 people don't mind. There are no ignorant people among the respondents.

Are you aware that your online activities (internet surfing, social media usage, online purchases) are tracked to create an online profile and send you advertisements?

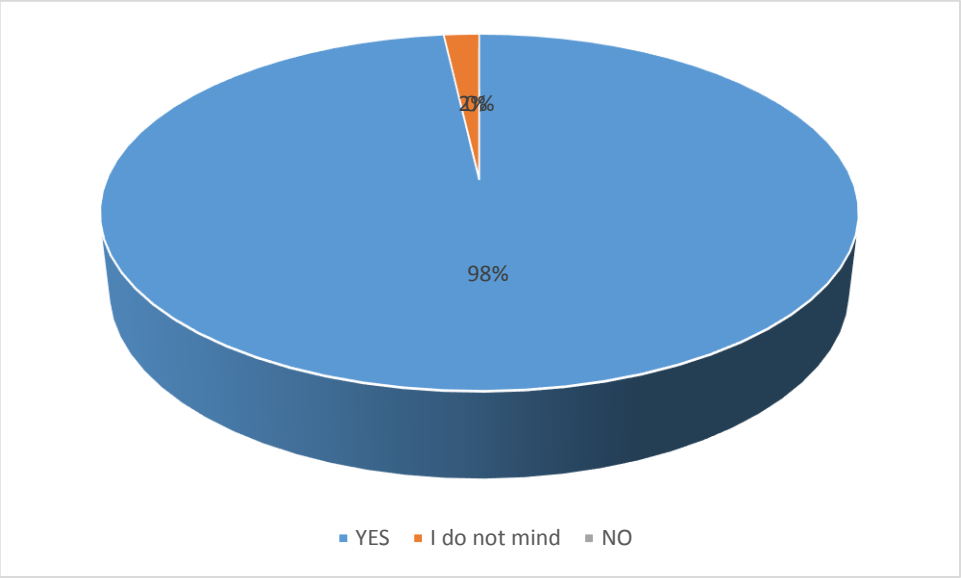

Figure 7. Respondents' awareness of creating an online profile and personalized ads.
Source: own elaboration.

Which of the following or used tools have you customized on your device?

The largest number of respondents (79 people) set privacy in social media. Nevertheless, 77 people track location and 76 installed an ad blocker. 70 people changed their passwords and 64 set the private mode in the web browser. 34 and 33 people deleted unused accounts and used anti-tracking tools. 3 people did not use any of the listed tools. Individuals applied DNS filtering through an external server.

How often do you change your e-mail password?

One of the questions that had the largest number of different answers concerned the frequency of password changes in e-mail.

Almost half, as many as 50 people, do not change their password in e-mail at all, they have the same password all the time. 36 people change their password once a year. 12 people change their password once a month. And the responses from individuals were as follows:

- Rarely.
- I prefer not to give.
- Every day.
- Quarterly.
- Once every 2 or 3 years, and if viruses are detected.
- Depends.
- If necessary.
- Every now and then.
- Once every 2 years.
- Every 3 months.
- once happened.
- From time to time, but not regularly.
- Mail has 2 passwords set by a program to create several hundred bit passwords.

40 people out of 111 were trained in cybersecurity, while as many as 71 people were not trained (Fig. 8).

Figure 8. Number of people trained in cybersecurity.

Source: own elaboration.

81 people expressed their willingness and interest in training in cybersecurity, the remaining 30 people do not see such a need (Fig. 9).

Figure 9. Number of people interested in cybersecurity training.

Source: own elaboration.

5. Conclusion

In recent years, the increasing use of the Internet has been observed. The Covid-19 pandemic has made people more willing to do various activities online, such as shopping. However, it carries many dangers that can cause many losses, not only financial.

Online threats are becoming more and more frequent, which is why it is so important to be aware of the threats lurking on the Internet, hence the idea of conducting a survey among the academic community.

Unfortunately, the reluctance to complete surveys, even short and anonymous ones, is still visible. Only 1/3 of the people answered the survey questions. On the other hand, as many as 70 out of 111 respondents were people aged 19-25, i.e. students.

Based on the survey, the following conclusions can be drawn:

- Most of the respondents knew forms of social engineering.
- Almost everyone has been in contact with a cyberattack and knows what it is.
- Respondents can indicate the form of a cyberattack.
- Respondents are aware of what they publish on the Internet.
- Respondents use various types of tools to protect their data.
- The problem among the respondents is low awareness of password change in e-mail.
- Most of the respondents do not change their password at all or do it very rarely.
- Most of the respondents (71) were not trained in cybersecurity.
- Most of the respondents (81) are interested in cybersecurity training.

The results of the research indicate that there is an increasing awareness of the community in the field of cybersecurity and the need for training in this field. It is a satisfactory fact that some people have already undergone such training, which proves that the employer cares about raising awareness of employees or the employees themselves have such a need.

Acknowledgements

The work was carried out as part of the Cyber Science postgraduate studies "Cybersecurity Management".

References

1. Broy, K., Drużyńska, L., Kiljan, A., Jonda, E. (2022). Koncepcja i znaczenie czwartej rewolucji przemysłowej. *Prace Katedry Materiałów Inżynierskich i Biomedycznych*. Politechnika Śląska, 38-50.
2. Cisowski, P., Ziemianin, A., Kiljan, A., Jonda, E., Spilka, M. (2021). Charakterystyka inteligentnej fabryki oraz wybranych filarów przemysłu 4.0. *Prace Katedry Materiałów Inżynierskich i Biomedycznych*. Politechnika Śląska,
3. Czekaj, F., Stecko, J. (2016). Cyberbezpieczeństwo a cyberprzestępczość. Kilka uwag na temat wyzwań współczesnego użytkownika Internetu. *Zeszyty naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie*, 24-34.
4. Dudzińska, A., Figielus, I., Jakubski, K., Trzyszka, J., Woźniak, N., Wyszomirska, W. (2020). *Ciemne strony cyberprzestrzeni – wybrane aspekty. Wyzwania i problemy społeczeństwa w XXI wieku*, 250-293.
5. Furmanek, W. (2012). *Zagrożenia wynikające z rozwoju technologii informacyjnych*. Uniwersytet Rzeszowski.
6. Garwol, K. (2018). Polska szkoła w dobie zagrożenia cyberprzestępczością. *Dydaktyka Informatyki, 13*. Uniwersytet Rzeszowski.
7. Gray, J. (2023). *Socjotechniki w praktyce. Podręcznik etycznego hakera*. Helion.
8. Gronowicz, G., Woś, M. (2018). Zagrożenia cyberterrorystyczne w świadomości młodzieży. *Edukacja Humanistyczna, 2*, 81-94.

9. Grubicka, J., Jopek, A. (2017). Tożsamość w cyberprzestrzeni: implikacje zjawiska cyberprzemocy wśród adolescentów. *Security, Economy & La,w XVII, nr 4*, 85-105.
10. Grubicka, J., Rogowski, K., Diemientiew, G. (2019). Dangers and attacks on digital information in the public safety space. Security Dimensions. *International and National Studies, 30*, 60-95.
11. Grzelak, M., Liedel, K. (2012). Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu. *Bezpieczeństwo Narodowe, nr 22, II*, 125-139.
12. https://ochronasieci.pl/zagrozenia-w-sieci/inzynieria-spoleczna/, 26.IV.2023.
13. https://payload.pl/usb-rubber-ducky/, 25.IV.2023.
14. https://www.bankier.pl/wiadomosc/Whaling-czyli-phishing-i-grube-ryby7292350.html, 25.IV.2023.
15. Jopek, A., Kinda, M. (2019). Cyber threats to a young internet user in the perspective of the development of the information society. *Security, Economy & Law, Nr 2(XXIII)*, 67-85.
16. Kowolik, S., Waniek, E., Kiljan, A., Jonda, E., Spilka, M. (2021). Kluczowe kompetencje Inżyniera Przemysłu 4.0. oraz charakterystyka wybranych filarów P4.0. *Prace Katedry Materiałów Inżynierskich i Biomedycznych*. Politechnika Śląska.
17. Kujawińska, I., Górecka, P., Kiljan, A., Spilka, M., Jonda, E. (2021). *Czwarta rewolucja przemysłowa, charakterystyka rozszerzonej rzeczywistości, cyberbezpieczeństwa oraz symulacji.* TalentDetector'2021 Summer. Prace Katedry Materiałów Inżynierskich i Biomedycznych, Politechnika Śląska.
18. Laskowski, P. (2008). *Bezpieczeństwo elektronicznych operacji bankowych*. Scientific bulletin of Chełm. Wałbrzyska Wyższa Szkoła Zarządzania i Przedsiębiorczości.
19. Lewandowska, A. (2019). Niebezpieczeństwa wynikające z korzystania z Internetu na komputerach i smartfonach. *Nowoczesne technologie XXI w. – przegląd, trendy i badania. Tom 1*.
20. Lizut, J. (ed.) (2014). *Zagrożenia cyberprzestrzeni*. Wyższa Szkoła Pedagogiczna im. Janusza Korczaka.
21. Noga, H., Małodobry, Z., Jarczak, J. (2018). Cyberprzestrzeń współczesnym miejscem przestępstwa. *Prace Naukowe Akademii im. Jama Długosza w Częstochowie. Technika, Informatyka, Inżynieria Bezpieczeństwa, t. VI*, 421-431.
22. Samociuk, D. (2023). *Antivirus evasion methods in modern operating systems*. Applied Sciences. Basel, 1-17.
23. Sikorska, A. (2022). *Ocena* wiedzy, umiejętności i postaw studentów Wydziału Filologicznego Uniwersytetu Łódzkiego w zakresie bezpiecznego korzystania z Internetu. *Acta Universitatis Lodziensis. Folia Librorum, 1*, 103-126.
24. Tomczyk, Ł. (2019). Problematyczne użytkowanie Internetu oraz portali społecznościowych wśród polskiej młodzieży. *E-mento, 2*, 44-54.

25. Walendzik, G., Wilkosz, K. (2018). Zapobieganie i przeciwdziałanie przemocy w cyberprzestrzeni. *Kontrola i audyt, Nr 1(styczeń-luty).*
26. Wawrowski, Ł., Białas, A., Kajzer, A. (2023). Anomaly detection module for network traffic monitoring in public institutions. *Sensors*, 1-18.
27. Wojtkowiak, M., Szumilas-Praszek, W. (2013). Internet jako współczesne medium zagrożenia czy edukacji. Rola Internetu w ponowoczesnym społeczeństwie. *Społeczeństwo i Rodzina, Nr 37,* 133-143.