Journal of Applied Technical and Educational Sciences
jATES
ISSN 2560-5429
http://jates.org

Cybersecurity awareness among university students

László Bottyán [1]

[1] *University of Pécs, Ifjúság útja 6, Pécs 7624 Hungary, laszlo@bottyan.com*

Abstract: *Due to the widespread integration of ICT in education, both the participants in the teaching-learning process and the educational institutions themselves have become increasingly susceptible to cyber threats. It is imperative to implement adequate protective measures for several compelling reasons. Information security awareness plays a pivotal role in the overall defense strategy. For this research paper, I evaluated the level of security awareness among a particular group of students. The results are consistent with the international research results. Among the findings, the two most problematic areas are password management and not performing sensitive activities other than our computer.*

Keywords: *information security; cybersecurity awareness; e-learning security; online threats*

1. Introduction

Cybersecurity awareness is briefly defined as "*the degree of users' understanding about the importance of information security, and their responsibilities to exercise sufficient levels of information control to protect the organization's data and networks*." (Shaw et al., 2009)

Rahim, Hamid, Kiah, Shamshirband, and Furnell concluded that cybersecurity awareness plays two significant roles: (i) alerting individuals using the internet about cybersecurity concerns and potential threats (ii) improving their comprehension of cyber threats, encouraging them to adopt security measures when using the internet wholeheartedly. (Rahim et al., 2015) The U.S. National Institute of Standards and Technology (NIST) distinguishes between awareness, training, and education. In their definition, learning is a continuum that starts with awareness, builds to training, and evolves into education. (Wilson et al., 2003) According to NIST Special Publication 800-16, awareness is defined as: "*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.*" (Wilson et al., 1998) For a successful increase of Awareness, Siponen highlights the importance of identifying, quantifying, and understanding the background for "human errors." In his concept, two categories relating to the problems of awareness are framework and content. The framework is more of an engineering discipline and a matter of explicit knowledge, while the content is a more informal interdisciplinary field of non-engineering.

Furthermore, the goal of increased awareness is to minimize the "user-related" faults and maximize the efficiency of security techniques from the user's perspective. (Siponen, 2000) Other studies assessed the users' consciousness based on a simple model that classifies the groups of users according to their skills and awareness: naive, typical, and conscious. Then, probabilities are assigned to each class, describing the likelihood of committing dangerous reactions in case of a cyber-attack. An interesting finding is that even with minor skill differences, making the users more conscious of their reactions can significantly enhance cybersecurity at a particular organization. (Hadarics et al., 2018; Bognár et al., 2018; Nagy et al., 2020)

The following outline will guide the remainder of the paper. In this paragraph, we will delve into the term cybersecurity awareness. Paragraph II will examine pertinent international studies regarding students' cybersecurity awareness. Paragraph III will focus on the cybersecurity awareness research conducted at the University of Dunaújváros, including its findings. The conclusions on the results will be presented in paragraph IV and some final thoughts in paragraph V.

2. International studies on university students' cybersecurity awareness

Al-Janabi and Al-Shourbaji conducted a 26-question survey in Middle Eastern higher education institutions in 2014. The research aimed to measure the level of information security awareness among teachers, university students, and employees (n=760)—questions covered areas such as email security, phishing, internet security, anti-virus programs, and data backups. The results showed that the participants need more knowledge in the daily practical application of information security principles. For example, the target groups must be aware of information security incidents and their consequences. (Al-Janabi, & Al-Shourbaji, 2016)

Moallem conducted a 10-question survey of students at two California state universities in 2017 and the first quarter of 2018 using the Qualtrics application (n=247). The goal was to assess the online security awareness of students studying in Silicon Valley, a highly technocratic environment. The results showed that although students know that Internet use can be traced and that their data is unsafe even on university systems, few use two-factor authentication or complex account passwords. Another finding was that educational institutions need to be more actively involved in raising students' awareness of, for example, how to protect themselves from a potential cyber-attack. (Moallem, 2019)

Senthilkumar and Easwaramoorthy investigated the cyber security awareness of university students in Tamil Nadu in 5 different cities in India – Chennai, Salem, Coimbatore, Vellore, Madurai (n=380). The goal was to measure students' security preparedness in 4 areas: virus attack, phishing, password strength, and abuse on the social network. The results showed that the student's exposure to the sources of danger appearing through social networks is the greatest. However, there is also a substantial deviation in the level of awareness related to passwords, so the authors point out that although the general information security awareness level is adequate, the mentioned areas need improvement. (Senthilkumar & Easwaramoorthy, 2017)

Mai and Tick's research compared the information security awareness, knowledge, and behaviour of university students in Hungary and Vietnam (n=313). The analysis was conducted using a questionnaire data collection method based on the answers of 313 university students in the two countries. The results showed that, regardless of the country, most students need more material knowledge about information security, and the practices used are also inadequate; for example, they ignore the security settings when using a smartphone. Based on the discussed research results, the authors emphasize the importance of formal security awareness education, which can directly support students in proper defense. (Mai & Tick, 2021)

Gabra et al. conducted a quantitative survey to identify students' awareness and enthusiasm to learn cybersecurity in Nigerian Universities (n=367). The results showed that university students need to gain basic cybersecurity knowledge. Among the questions is that of password management result analysis, which shows 204 said No, 139 said yes, and 22 said maybe to using hard-to-guess passwords. Regarding the question on opening an email sent from an unfamiliar person, the result shows that 219 said yes out of 367, 110 said no, and 36 said maybe. This result indicates that most students need to learn about phishing attacks. (Gabra et al., 2020)

In conclusion, these studies underscore the global significance of enhancing cybersecurity awareness within educational institutions. Addressing these issues is crucial to prepare students, teachers, and employees better to navigate the digital landscape securely and protect sensitive information in an increasingly interconnected world.

3. Cybersecurity awareness research at the University of Dunaújváros

3.1. Background

Studies consistently show that students from diverse backgrounds who use the internet and computers often have limited awareness of cybersecurity risks. Moreover, there is no standard way to evaluate the viewpoints and preferences of online users on cybersecurity measures. To address this gap, Erol et al. developed a comprehensive scale to assess internet users' attitudes and behaviours related to cybersecurity. The validity of this scale was examined through factor analysis, resulting in the emergence of the "Personal Cyber Security Provision Scale." This scale comprises five distinct factors and demonstrates strong compatibility and reliability, making it a valuable tool for assessing users' perceptions and practices in cybersecurity. (Erol et al., 2015)

3.2. Methodology

The Personal Cyber Security Provision Scale (PCSPS) questionnaire consists of 25 questions grouped by the following categories: Protecting privacy (10 questions); Avoiding the untrusted (4 questions); Precaution (5 questions); Protection of payment information (2 questions); Leaving no trace (4 questions). All questions are straight, except the group protecting privacy, which are reversed. The answer options are 1 to 5 on a Likert scale in the following order: 1-Never, 2-Rarely, 3-Sometimes, 4-Often, 5-Always. The questionnaire consists of 5 additional questions on top of the PCSPS originals. Three are related to gender, age, and the field of studies; the last two are related to general safety in cyberspace. For data collection, Google Forms was utilized, while analysis was done using IBM SPSS Statistics v25.

3.3. Participants and sampling

The target population consisted of undergraduate students at the University of Dunaújváros. Due to the study’s exploratory nature, convenience sampling was used to recruit students from the entire university, irrespective of their course. Participants recruited were pursuing a university degree in seven fields of study to increase the variability of the sample: IT, and Engineering. A total of 15 students participated in this research, 12 male and 3 female. From the study field perspective, 13 respondents came from the technical area and 2 from the informatics area.

3.4. Results

The questions about data protection were reversed, leading to reversed results. The median score was 4 on the 5-point Likert scale (Table 1, Diagram 1); most affirmative answers were given to the statement "I share my personal information on the internet, when necessary" and the combined password-related statements of "I set easy to remember passwords," and "I make sure all my internet passwords are the same." Respondents often use easy-to-remember passwords to access multiple services, which puts them at risk for simultaneous attacks if any one account is compromised.

The median score was 4 on the 5-point Likert scale regarding avoiding the untrusted. (Table 1, Diagram 1) However, the "I do not accept friend requests from strangers on social media" statement received the least positive responses. We must be cautious when accepting social media requests from unknown individuals, as it can lead to spam, scams, and cyberbullying.

The precaution area scored 3.8 out of 5 on the Likert scale. (Table 1, Diagram 1) The statement that received the least number of affirmative responses was "I change web browser security settings". It is important to note that unknown or uncontrolled browser settings can lead to various risks, such as malicious extensions, online activity tracking, and automatic data storage of cookies and other personal information.

The lowest median score of 2.5 on a 5-point Likert scale is linked to payment information protection. (Table 1, Figure 1) The respondents revealed that they conduct their banking and online shopping from sources other than their computers. This practice increases the risk of data compromise due to unknown security settings, unauthorized or malicious software, viruses, or other hidden harms associated with that specific computer.

The score for leaving no trace is the second lowest, at 3.5 out of 5. (Table 1, Figure 1) According to a survey, people were least likely to agree with the statement, "I change my passwords regularly while using the internet." This presents a potential risk as if the computer is lost or stolen, and the old passwords could still be revealed, which puts the user's accounts at risk. Additionally, unchanged passwords could make it challenging to discover if the account has been compromised.

Table 1. Descriptive statistics of the cybersecurity awareness research at University of Dunaújváros.

	Protecting privacy INV	Avoiding the untrusted	Precaution	Protection of payment information	Leaving no trace
N	15	15	15	15	15
Mean	3,9067	3,6	3,6933	2,6333	3,55
Std. Deviation	0,53648	1,18322	0,5175	1,27429	0,59911
Median	4	4	3,8	2,5	3,5
Minimum	2,7	1	2,6	1	2,25
Maximum	4,8	5	4,2	5	4,5

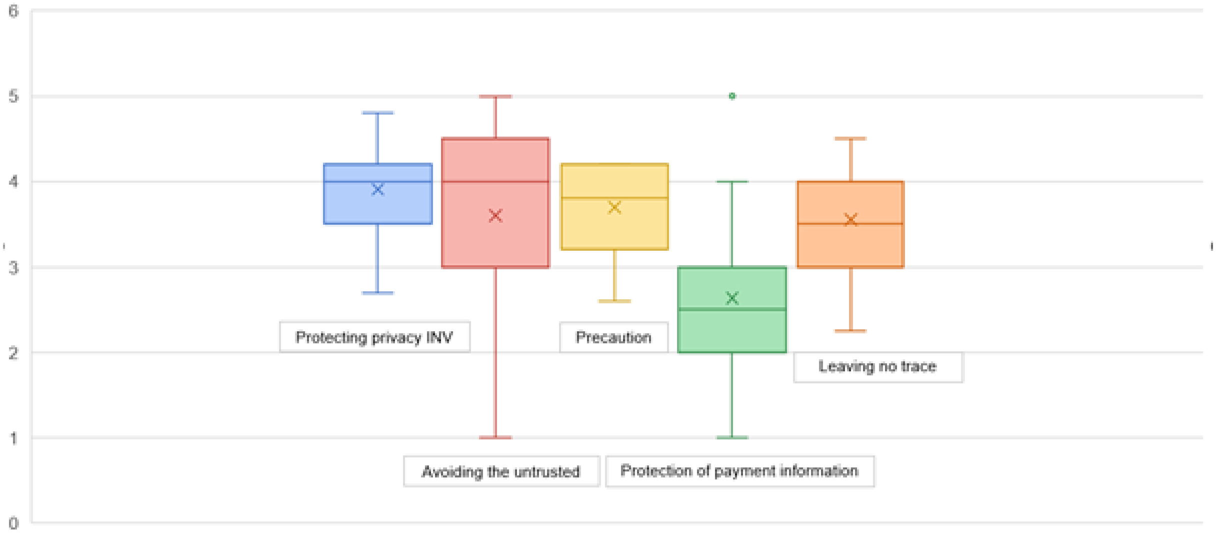

Figure 1. Box plot of the cybersecurity awareness research at University of Dunaújváros.

In response to the statement, "I feel generally safe in cyberspace," 73.3% of respondents answered yes or mostly yes. However, this also means that over a quarter of respondents do not or mostly do not feel safe in cyberspace. (Table 2, Figure 2)

Table 2. I feel that I am generally safe in the cyberspace.

Answer	Frequency	Percent	Valid Percent	Cumulative Percent
No, not at all	1	6.7	6.7	6.7
Mostly no	3	20	20	26.7
Mostly yes	8	53.3	53.3	80
Yes, fully	3	20	20	100
Total	15	100	100	

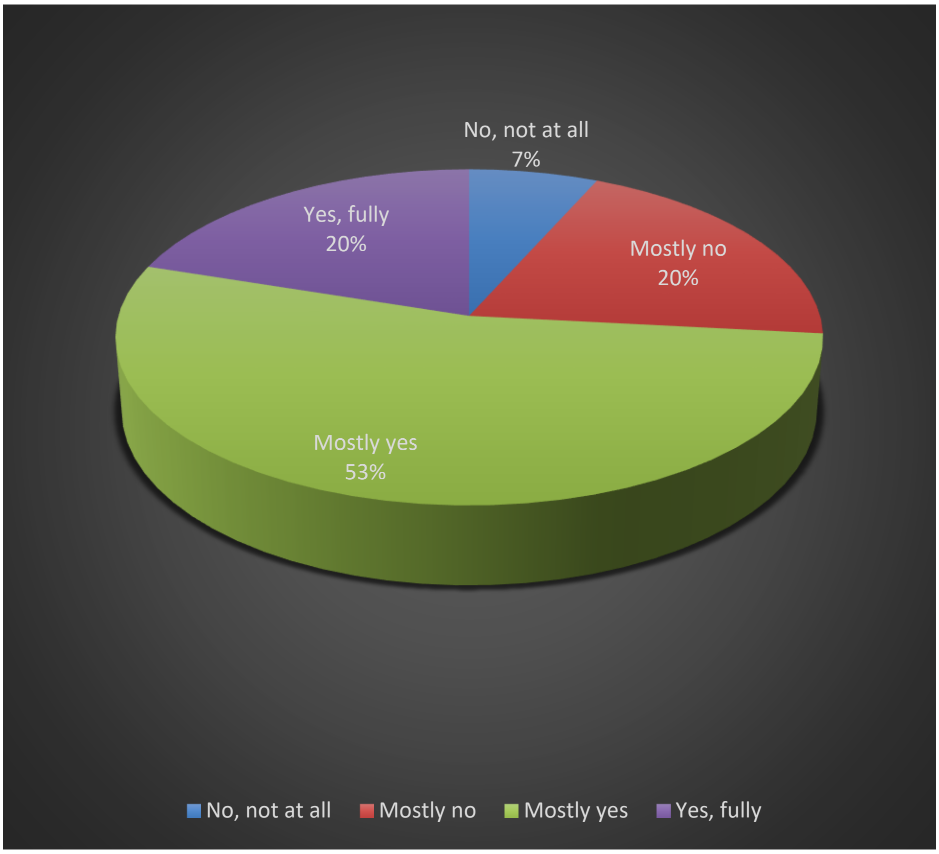

Figure 2. I feel that I am generally safe in the cyberspace.

According to the survey, 53.3% of individuals claimed to have never experienced any information security incident, such as hacking, fraud, online abuse, harassment, or virus/ransomware attack. However, the remaining 46.7% of respondents stated that they have been a victim of such an attack at least once. (Table 3, Diagram 3)

Table 3. I have been the victim of an information security incident (fraud, hacking, harassment, online abuse, virus / ransomware attack, etc.)

Answer	Frequency	Percent	Valid Percent	Cumulative Percent
Never	8	53,3	53,3	53,3
1 or 2 times in my life	6	40	40	93,3
It has happened 3 or more times	1	6,7	6,7	100
Total	15	100	100	

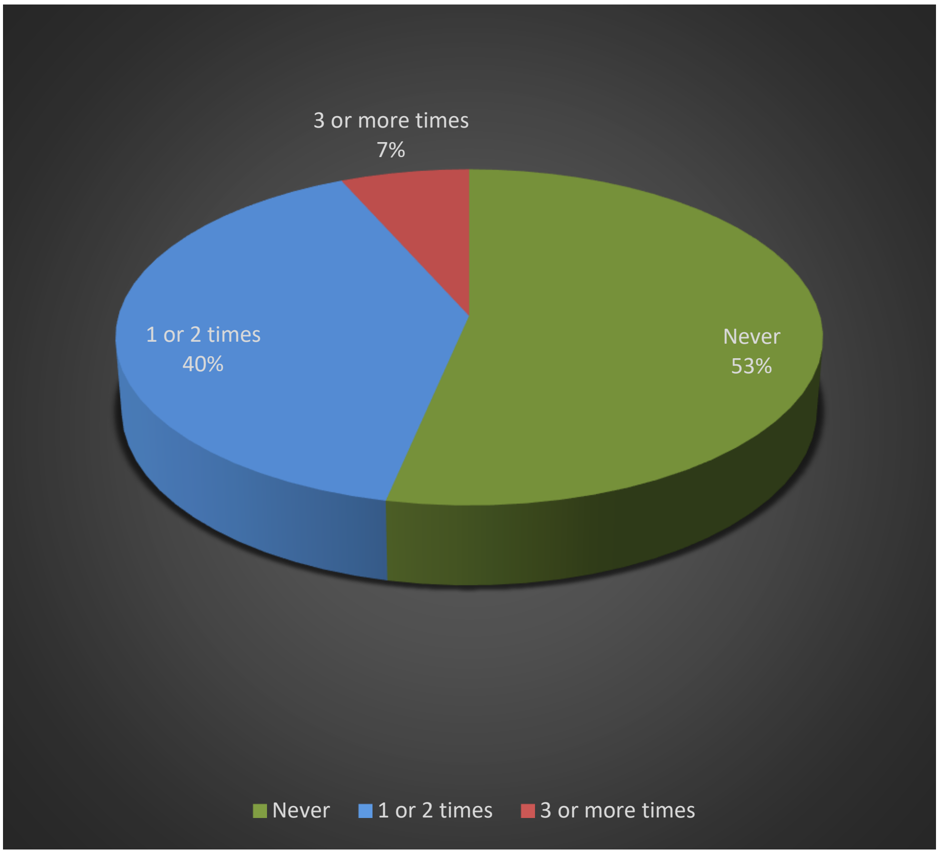

Figure 3. I have been the victim of an information security incident in my life.

4. Discussion

Teachers, students, and schools are more vulnerable to cyberattacks due to the increased reliance on digital tools and platforms for teaching and learning. The teaching-learning process participants must be adequately trained because a lack of awareness can result in risky online behaviors that make them more susceptible to cyber threats. It should also be considered that inappropriate safety-conscious behaviour can affect individuals and an entire educational institution.

This research was prepared only for a small group of students from a single institution. However, it fits in with the results of international research from the point of view of the need to increase general security awareness (Al-Janabi & Al-Shourbaji, 2016; Moallem, 2019; Mai & Tick, 2021). Among the findings, the two most problematic areas are password management and not performing sensitive activities other than our computer.

A further research opportunity is to compare the obtained results with data collected in a broader sample. On the other hand, the security awareness of instructors and the information security organization of educational institutions.

5. Conclusion

This sample shows that a limited group of students at the University of Dunaújváros can be considered more aware of information security in the light of the examined areas, but there are exceptions to the trend. The average age of the respondents was 20.73. One problematic area is that the responding students typically bank or shop online from other computers that are not their own. Although it cannot be clearly stated that this carries a high risk in every single case, it is still possible that the workstation in question has lower security settings or, for example, is already infected or activities can be tracked on it, and is, therefore, more likely to be considered dangerous. The development of competences and a better knowledge of technological solutions can help identify threats more effectively (Demeter & Kővári, 2020).

Another group of potential risks tends towards passwords. Respondents often use the same password for multiple services, use easy-to-remember passwords, and change their Internet passwords less frequently. These results are consistent with the international research results mentioned at the beginning of this study i) Moallem's findings that despite students knowing the Internet's risks, they still use low security measures, e.g., complex passwords even on public university systems (Moallem, 2019) ii) Senthilkumar and Easwaramoorthy found that there is a variance in awareness levels related to passwords (Senthilkumar & Easwaramoorthy, 2017) iii) Gabra et al. found that only a minority of respondents use hard-to-guess passwords. (Gabra et al., 2020). Farkas et al. (2014) are concerned with the secure and efficient transmission of data in sensor networks, the educational research emphasizes the need for secure digital platforms for teaching and learning. Both could benefit from the integration of secure protocols and systems.

Finally, an attention-grabbing result is that half of the respondents have already been victims of an information security incident, and a quarter do not feel safe on the internet. This is a growing concern as instances of online harassment are on the rise. According to a study by Lindsay and Krysik, the rate of online harassment has more than doubled since Finn's study in 2004. The Annenburg Public Policy Center also found that 43.3 percent of individuals have experienced online harassment, compared to 16.2 percent and 15.8 percent in previous studies. (Lindsay & Krysik, 2012).

References

Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information & Knowledge Management, 15(01), 1650007. https://doi.org/10.1142/s0219649216500076

Bognár, L., Jóos, A., & Nagy, B. (2018). An improvement for a mathematical model for distributed vulnerability assessment. Acta Universitatis Sapientiae, Mathematica, 10(2), 203–217. https://doi.org/10.2478/ausm-2018-0017

Demeter, R., Kővári, A. (2020). Importance of digital simulation in the competence development of engineers defining the society of the future. CIVIL SZEMLE, 17(2), 89–101.

Erol, O., Şahin, Y., Yılmaz, E., & Haseski, H. (2015). Personal cyber security provision scale development study kişisel siber güvenliği sağlama ölçeği geliştirme çalışması. International Journal of Human Sciences, 12, 75. https://doi.org/10.14687/ijhs.v12i2.3185

Farkas I. et al (2014). Wireless Sensor Network Protocol Developed for Microcontroller-based Wireless Sensor Units, and Data Processing with Visualization by LabVIEW. In 2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI). pp. 95–98.

Garba, A., Maheyzah Binti Sirat, Siti Hajar, & Ibrahim. (2020). Cyber Security Awareness Among University Students: A Case Study. Sci Prcd Ser, 2(1), 8286. https://doi.org/10.31580/sps.v2i1.1320

Hadarics, K., Győrffy, K., Nagy, B., Bognár, A., Arrott, A., & Leitold, F. (2018). Mathematical Model of Distributed Vulnerability Assessment In: Jaroslav, Dočkal; Milan, Jirsa; Josef, Kaderka (szerk.) Proceedings of Conference SPI 2017: Security and Protection of Information

Brno, CZ: National Defence University (Brno) (2017) pp. 45-57, 13 p.

Lindsay, M., & Krysik, J. (2012). ONLINE HARASSMENT AMONG COLLEGE STUDENTS. Information, Communication & Society, 15(5), 703–719. https://doi.org/10.1080/1369118X.2012.674959

Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. Acta Polytechnica Hungarica, 18(8), 67–89. https://doi.org/10.12700/aph.18.8.2021.8.4

Moallem, A. (2019). Cyber Security Awareness Among College Students. In Ahram, Tareq Z & D. Nicholson (Eds.), Advances in Human Factors in Cybersecurity (pp. 79–87). Cham: Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-94782-2_8

Nagy, B., Joós, A., & Bognár, L. (2020). Assessing the effect size of users' consciousness for computer networks vulnerability. Acta Universitatis Sapientiae, Mathematica, 12(1), 14–29. https://doi.org/10.2478/ausm20200002

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in tamil nadu. IOP Conference Series: Materials Science and Engineering, 263, 042043. https://doi.org/10.1088/1757-899X/263/4/042043

Shaw, R.-S., Chen, C., Harris, A., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52, 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Siponen, M. (2000). Siponen, M.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8(1), 31-41. Inf. Manag. Comput. Security, 8, 31–41. https://doi.org/10.1108/09685220010371394

Wilson, M., & Hash, J. (2003, October 1). Building an Information Technology Security Awareness and Training Program (NIST, Ed.). Retrieved from csrc.nist.gov website: https://csrc.nist.gov/pubs/sp/800/50/final

Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. Education and Information Technologies, 26(2), 1721–1736. https://doi.org/10.1007/s10639020103300

Wilson, M., Pitcher, S., Tressler, J., Ippolito, J., & deZafra, D. (1998, April 1). Information Technology Security Training Requirements: a Role- and Performance-Based Model. Retrieved from csrc.nist.gov website: https://csrc.nist.gov/pubs/sp/800/16/final

About Authors

László BOTTYÁN is a PhD student at the „Education and Society" Doctoral School at the University of Pécs. He absolved his master's studies at the Budapest University of Technology and Economics. His research focuses on the cybersecurity aspects of digital learning.