Volume 14, Number 1, 2024
14. kötet, 1. szám, 2024
https://doi.org/10.24193/PedActa.14.1.6

ON THE FACTORS OF STUDENTS' CYBERSECURITY BEHAVIOR

Gabriella ROSTA, László BOTTYÁN, László BOGNÁR

Abstract: The article is an exploratory research on the security awareness of university students in the light of various sociodemographic factors. Information technology, and information security in particular, plays a critical role in this context. Awareness is a fundamental component of security preparedness because it empowers individuals to recognize and respond to security threats and fosters a security culture. By educating students and teachers about the importance of security and best practices, educational organizations can significantly enhance their overall security posture. The article points out that raising awareness of information security is not a simple task and requires a systematic approach. In this respect, education has both the potential and the responsibility to develop an information security mindset. The results of the article show that although the average response value of 3.735 suggests a security-aware attitude, the significant difference between the minimum and maximum values indicates a high variability. Looking in more detail at information security factors, the article reveals that law students are more cautious about protecting personal data, while IT and engineering students are more open to online banking and shopping.

Keywords: cyber security, higher education, security awareness, case study, online threats

1. Introduction

Education serves as the fundamental basis for the revitalization and alteration of our societies. It harnesses knowledge to assist us in navigating a world that is constantly changing and unpredictable. The potency of education resides in its ability to establish connections between individuals and the world, enabling us to transcend our current boundaries and explore new opportunities. It fosters a sense of unity among us, encourages collaborative efforts, and equips us with the scientific expertise, knowledge, and innovation necessary to tackle shared obstacles. Education cultivates comprehension and develops skills that can contribute to the creation of a future that is more inclusive, equitable in terms of economics, and sustainable in relation to the environment. (UNESCO, 2021)

Young students' physical worlds quickly shrank as personal meetings and activities were restricted at the beginning of COVID-19, but their online worlds grew at a similar rate. They felt absolutely comfortable when they interacted with others on the internet and for them, there is little difference to in-person interactions. UNICEF warned that children were at huge risk of hurt during the epidemic in the spring of 2020 (UNICEF, 2020) because of the dramatic increase in their on-screen moments as their lives moved online to study and maintain social ties with their friends and family members.

We are all aware of how quickly technology advances. It's simple to get sucked into the newest, greatest applications and online trends because they appear frequently. Given the pandemic situation's lack of social opportunities and physical activities, that had undoubtedly been amplified. UNICEF was concerned that young pupils' magnified use of technology might expose them to more online harmful content or encourage risk-taking behaviors like approaching strangers or getting sucked into dangerous activities. (UNICEF, 2020)

Technology is used in schools to take care of and help students as they get in touch with the online world. As required by the Children's Internet Protection Act, schools will have appropriate tools for monitoring and filtering in the classrooms, and some of them can use keyword analysis to help spot the newest trends. This will allow school instructors to keep an eye on any potential activity related to a variety of e-safety topics, such as bullying, radicalization, terrorism, child sexual exploitation, and others. (Hinckley, 2002)

Received

To keep students safe, it's important to avoid simply limiting access to everything, as this would prevent them from learning. Rather, schools can make use of technology to create a secure online setting where students can practice the skills, they have already learned about communicating with others online. Some school-based e-safety explanations even let users set age-appropriate usage restrictions, giving students the possibility to learn and, more importantly, make mistakes without fear.

But things have changed now when students are studying at home. The same support and filtering may be provided if they are using a computer provided by the school, but most of the students will surely be using personal or domestic devices without these protections. Thus, having the information necessary to make wise choices regarding online safety is essential.

Starting in primary school and continuing throughout the student's years in school and beyond, educators should prioritize imparting students with the necessary knowledge and competencies to exercise responsible internet usage. These abilities include the capability to search for information, find it, and determine its veracity and accuracy. Students must have these skills to take control of their online worlds and make wise decisions when interacting with others, making digital life an essential component of education, principally in today's context.

There is a lot to learn, and institutes need to cover all of it. A similar set of social norms for online interaction exists, sometimes called the "nine elements of digital citizenship," just as we learn the social protocols for interacting in person. Digital access, digital commerce, digital communication, digital literacy, digital etiquette, digital law, digital rights and responsibilities, digital health and wellness, and digital security are among the topics they cover. (Ribble, 2015)

Involving instructors in these categories will guarantee that children have a thorough comprehension of what it is to take part in the online society, and outstanding resources are available to assist teachers in doing this. Certain schools have also had good experiences with peer-led initiatives, which give students the tools to educate their mates about online safety and keep themselves safe while doing so.

Certainly, staying current with trends is essential, so teacher training should be kept up to date and resource validity must be regularly examined. Regardless of the age group, it will be important to emphasize important online safety messages frequently enough to stick in students' minds. Through this, we can hope that students will be able to responsibly use technology.

The involvement of parents and other caregivers is a further effective method in the teaching of prudent internet use. Parents who participate in their kids' online occupation from a young age are in a great position to discuss with their kids the apps they are using and why, and to mentor them as they grow. Parents need all the assistance they can receive to follow the rapidly changing environment, which puts them in a better position to be aware of any potential threats that their kids may be encountering.

The only method to guarantee that kids know necessary to inquire, investigate, and form their own opinions about what is true or safe online is through ongoing learning. To make the most of the internet while staying safe, it's important to reinforce those fundamental safety messages and keep up with current online trends and their potential effects.

Each of us is continually learning. We can't protect our children from all risks, but we can equip them with the knowledge and resources to help them come to the best decisions possible.

In an effort to comprehend the degree of information security awareness, the related risks, and the overall influence on schools, several research (Al-Janabi & Al-Shourbaji, 2016; Aloul, 2012; Eyadat, 2018) have been made within educational environments in the Middle East. The findings show that none of the participants—educators, researchers, students, and employees—has the necessary knowledge and comprehension of the significance of information security principles and how they can be applied practically in their daily work.

According to research, Muslim students in the Middle East are regularly bringing their smartphones to the physical or online classroom, which has important security problems, especially if they are not as aware of the risks to device information security. The results of the different studies revealed that although students had a strong understanding of most information security notions when speaking about their computers, they became less aware of their smartphones' protection (Al-Janabi & Al-Shourbaji, 2016). In light of the research

results, it would be possible to give well-founded feedback to the heads of the institutions, on the one hand, and to the education administration, on the other hand, about what remedial measures are necessary to improve cyber security, protect data, prevent cyber threats, and raise the security level of the learning environment supported by digital devices.

2. Methods

The target population consisted of undergraduate international students from several countries at two universities in Hungary. Due to the study's exploratory nature, convenience sampling was used to recruit students from both universities, irrespective of their course. Participants recruited were university students in several fields of study to increase the variability of the sample: Law, Social sciences, IT, and Engineering. A total of 73 students participated in this research, 39 male and 34 female. From the study field perspective, 13 respondents came from the Informatics field, 36 from Law, 4 from the technical area, and 20 from the social sciences.

The measure we used is based on Erol and colleagues' use of factor analysis to introduce a comprehensive scale designed to evaluate the attitudes and behaviors of internet users about cybersecurity called the "Personal Cyber Security Provision Scale" (PCSPS). The PCSPS questionnaire comprises 25 questions in five groups relating to the five underlying factors. Protecting privacy factor with 10 questions, Avoiding the untrusted factor with 4 questions, Precaution factor with 5 questions, Protection of payment information factor with 2 questions, and Leaving no trace factor with 4 questions. (Erol et al., 2015) The measurement was made using a 5-point Likert scale.

In addition, the questionnaire consists of 5 additional questions related to gender, age, the field of studies, and general safety in cyberspace. Google Forms was used to collect data, and for data analysis IBM SPSS Statistics v25 and Minitab v21 were applied.

3. Results

The aggregated results show a varied picture. The mean value of 3.735 for the answers shows that the respondents prefer to follow a safety-conscious attitude. However, at the same time, the range suggests that the variability is high. (Table 1)

Table 1. Summarized item statistics.

	Mean	Min	Max	Range	Max/Min	Variance
Item Means	3.735	2.559	4.721	2.162	1.845	.372
Item Variances	1.369	.485	2.668	2.183	5.498	.387

In what follows we introduce some detailed results. If we look through the factors, Leaving No Trace received the lowest mean among the five factors examined. It means that the respondents pay less attention to security on foreign computers. The second lowest mean was for the Precaution factor. Respondents least often check the safety of the connection and the web pages. The highest mean received for the Protection of payment information. The questioned students are more cautious of internet banking and online shopping. The second highest factor value is Avoiding the untrusted. The respondents are more likely to check the source of information before they act on the internet. (Table 2)

Table 2. Descriptives of Factors

					95% Confidence Interval for Mean	
Factor	**N**	**Mean**	**Std. Dev.**	**Std. Err.**	**Lower Bound**	**Upper Bound**
Privacy	72	3.67	1.125	.133	3.40	3.93
Avoiding	73	3.79	1.169	.137	3.52	4.07
Precaution	71	3.53	.686	.081	3.36	3.69
Payment	71	3.99	.479	.057	3.88	4.11

Trace	72	3.33	.708	.083	3.17	3.50
Total	359	3.66	.902	.048	3.57	3.76

Detailed results of the Protecting privacy factor can be summarized in Table 3 using the Likert scale 1-Never, 2-Rarely, 3-Sometimes, 4-Often, 5-Always. Within the protecting privacy factor, the two password-related statements, "I make sure all my internet passwords are the same" and the statement "I set easy to remember passwords" received the lowest reversed mean score. All of this means that respondents sometimes set the same password for multiple Internet accounts and usually use passwords that are easy to remember. Using easy or uncomplicated passwords can make it easier for hackers to guess them. When the same password is employed across multiple accounts, it increases the vulnerability of numerous accounts and personal information to potential compromise. (Table 3)

Table 3. Item statistics: Protecting privacy.

Statement	Mean	St. Dev.	N
I make sure all my internet passwords are the same	3.12	1.072	68
I reply to authentication messages (requests such as username, password, etc.) received by e-mail	3.60	1.437	68
I communicate with people I don't know using a webcam	4.72	.770	68
I share my personal information (Identity no, Date of birth, GSM no etc.) on the internet, when necessary	3.44	1.151	68
I open email attachments from people who I do not know	4.53	.762	68
I share my personal information on social networks	4.22	.844	68
I declare my location on the internet	4.44	.817	68
I shop by clicking the ads on social networks	4.40	.813	68
I set easy-to-remember passwords	3.21	1.059	68
I respect and respond to e-mails (requests such as card numbers, passwords, etc.) from sites such as banks, online shopping sites, etc.	4.28	1.104	68

Detailed results of Avoiding the untrusted factor can be summarized in Table 4 using the Likert scale 1-Never, 2-Rarely, 3-Sometimes, 4-Often, 5-Always. Within the Avoiding the untrusted factor, the lowest mean received to the statement "I do not accept friendship requests from people I do not know on social networks"; this means respondents may increase the risk of scammers by befriending strangers and sharing personal information. The questioned students, however, often ignore online money and credit requests. (Table 4)

Table 4. Item statistics: Avoiding the untrusted

Statement	Mean	St. Dev.	N
I ignore online money and credit requests	4.07	1.308	68
I do not accept friendship requests from people I do not know on social networks	3.34	1.599	68
I do not subscribe to websites that I do not trust	3.75	1.633	68
I do not download files from websites that I do not trust	3.57	1.529	68

Detailed results of the Precaution factor can be summarized in Table 5 using the Likert scale 1-Never, 2-Rarely, 3-Sometimes, 4-Often, 5-Always. Within the Precaution factor, the lowest mean was received to the statement "I change web browser security settings". Unchanged browser security settings could lead to threats of unblocked popups, unwanted data collections, and malicious extensions. Most of the respondents, however, often have antivirus installed on their computers. (Table 5)

Table 5. Item statistics: Precaution

Statement	Mean	St. Dev.	N
I check connection security (https://) and certificates on web pages	3.18	1.292	68
I update the software that I use	3.65	1.156	68
I have antivirus software on my computer	4.07	1.188	68
I avoid using weak passwords	4.00	.898	68
I change web browser security settings	2.78	1.268	68

Detailed results of the Protection of payment information factor can be summarized in Table 6 using the Likert scale 1-Never, 2-Rarely, 3-Sometimes, 4-Often, 5-Always. As discussed in the beginning of this

chapter, the factor protection of payment information has the highest average score of all factors. The results of the two questions are very close to each other; the respondents often use their personal computers for banking and online shopping. Foreign computers' security settings are usually unknown; therefore, doing sensitive activities such as online shopping or banking increases the risk of user ID or password theft, hacking, and gaining unauthorized access. (Table 6)

Table 6. Item statistics: Protection of payment information

Statement	Mean	St. Dev.	N
I conduct internet banking transactions using my personal computer.	3.79	1.241	68
I shop online using my personal computer.	3.88	1.252	68

Detailed results of the Leaving no trace factor can be summarized in Table 6 using the Likert scale 1-Never, 2-Rarely, 3-Sometimes, 4-Often, 5-Always. Within the factor leaving no trace, the statement "I change the passwords that I use on the internet" and "I delete web browser history" received the lowest mean score. The respondents only sometimes pay attention to the traceability of their activity. Left browser data could lead to cookie theft, which is used by cybercriminals to steal and use them to gain access to sensitive information. (Table 7)

Table 7. Item statistics: Leaving no trace.

Statement	Mean	St. Dev.	N
I pay attention not to store my personal information on computers other than my personal computer.	4.69	.697	68
I delete web browser history.	2.82	1.158	68
I log out of my accounts such as social media, e-mail when I finish my work.	3.26	1.431	68
I change the passwords that I use on the internet.	2.56	1.028	68

The questionnaire asked what field the person filling in is studying: 1-IT, 2-Law, 3-Technology, 4-Social. The mean results are different by study field. In the privacy factor, the reversed lowest mean score from the technology students means they are less cautious about protecting their personal data. The highest score acquired from law students shows that they pay more attention to protecting their personal data. (Figure 1)

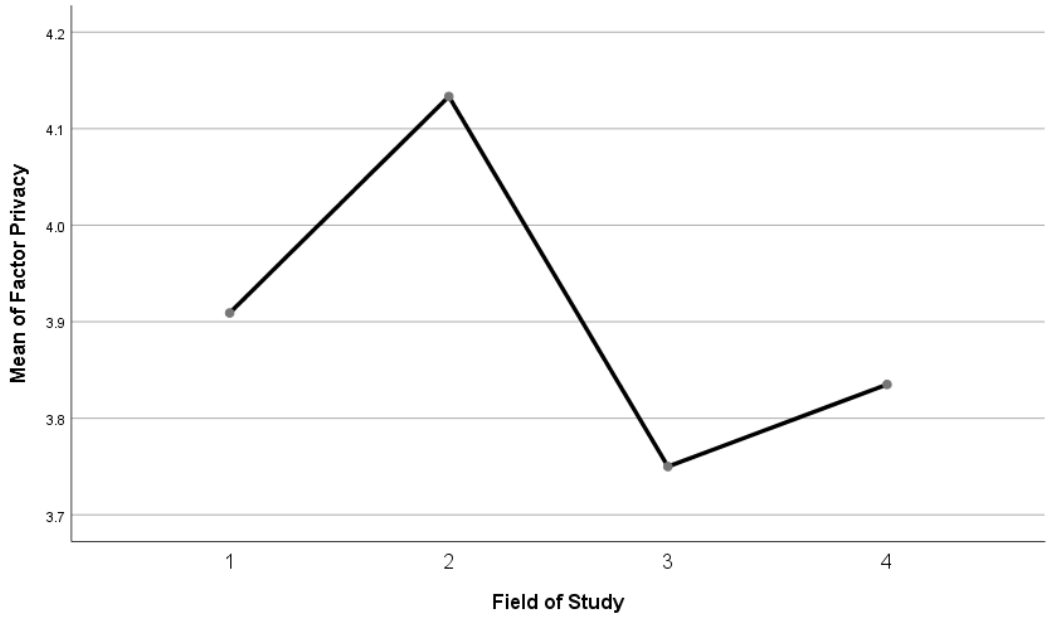

Figure 1. Means of factor privacy per field of study of the respondents.

Within the Avoiding the untrusted factor, the lowest mean again from the technology students means they're less often paying attention to trusted sources and trusted people. However, IT, law, and social students are more cautious about untrusted websites, downloads, and requests from unknown people. (Figure 2)

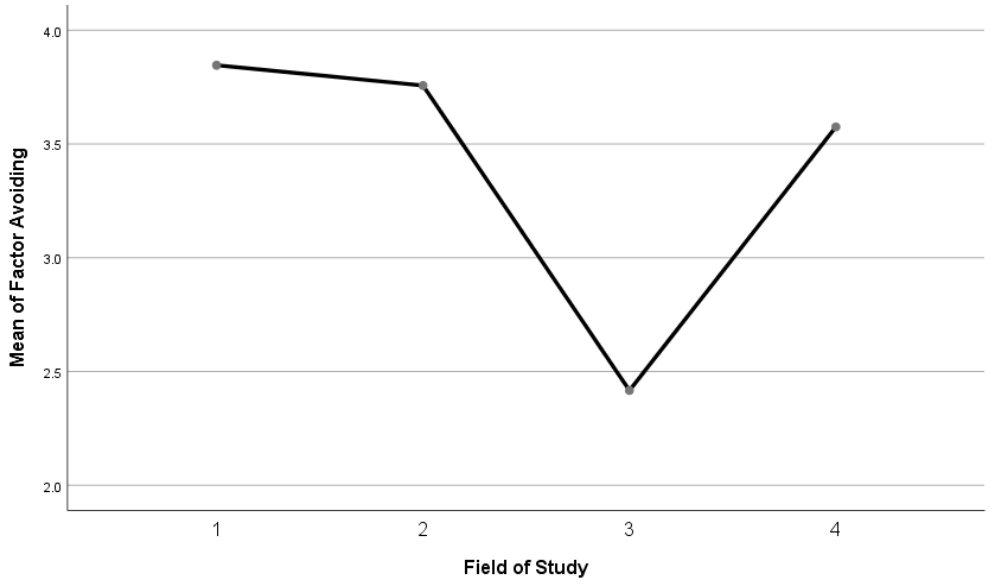

Figure 2: Means of factor avoiding the untrusted per field of study of the respondents.

In the Precaution factor, each field of study achieved different results. As previously discussed, this factor produced the second weakest results and should not be overlooked. By the field of study, IT students are the most cautious of software updates, antivirus, browser, or connection settings, while this decreases among law and engineering students. Social students pay the slightest attention to the mentioned computer security settings. (Figure 3)

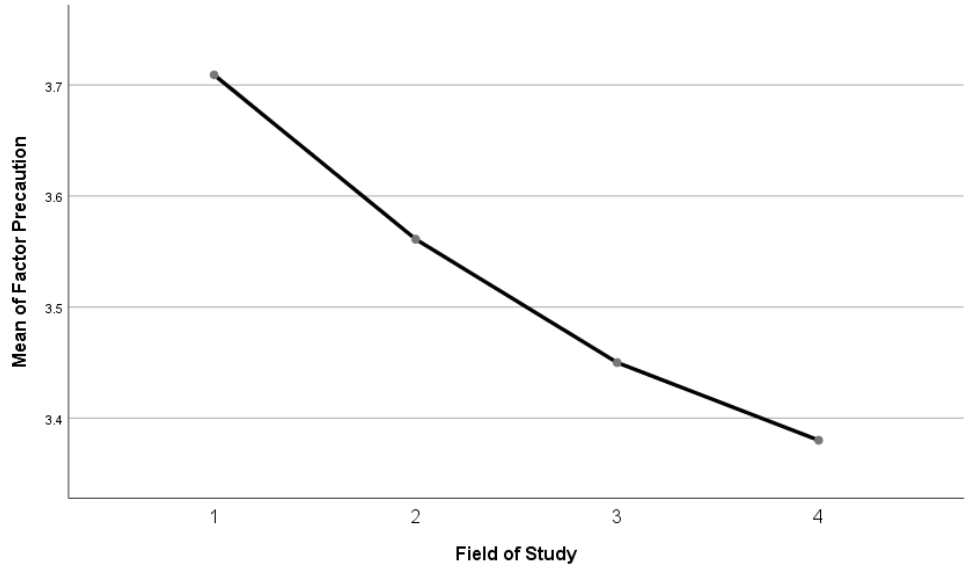

Figure 3: Means of factor precaution per field of study of the respondents.

The results are various within the Protection of payment information, which has the strongest results with the highest mean from all factors. By the field of study, the law and social students fall into the higher mean scores, meaning they often conduct internet banking and online shopping from their computer, while the IT

and technology students are the opposite; they are more open to doing such activities on foreign computers. (Figure 4)

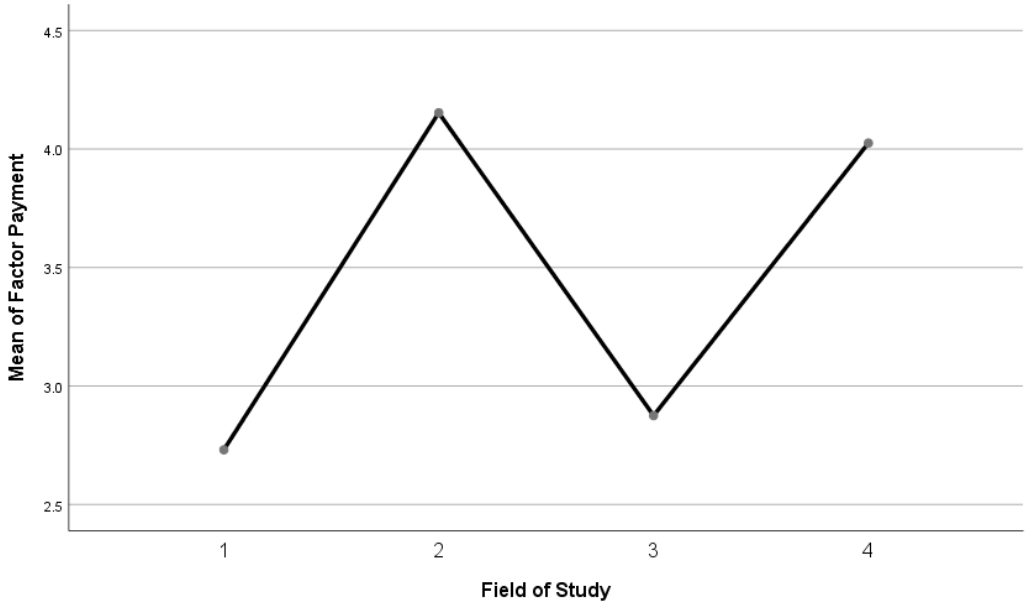

Figure 4: Means of factor protection of payment information per field of study of the respondents.

Leaving no trace has the lowest mean score of all factors. The results of the study field show that IT students pay more attention to not storing personal information, deleting browser history, or logging off from social accounts on foreign computers. Technology, law, and social students are less cautious about these activities. As discussed previously, there are several risks associated with this behavior because we are unsure about the foreign computer security settings. (Figure 5)

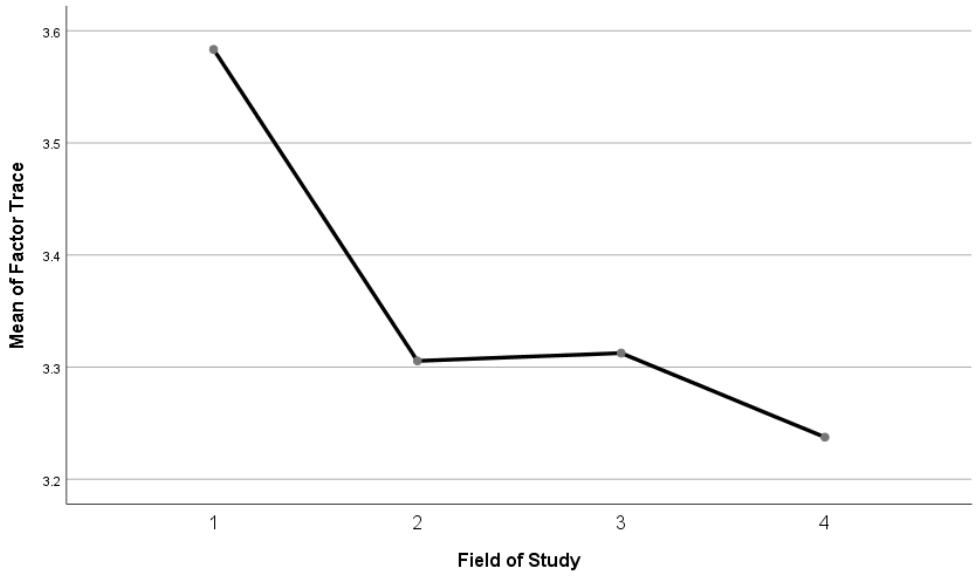

Figure 5: Means of factor leaving no trace per field of study of the respondents

4. Discussion

Among the questions, statements related to the web browser received the lowest mean values, which contributed to Precaution and Leaving no trace finishing last among the factors. It is a fact that this also requires adequate technical knowledge to know where to change the settings of the browser programs and delete the history. It is, therefore, not surprising that IT students are often more cautious than other students in both factors when broken down by field of study.

The second lowest median value was given to statements related to passwords, which, together with the previously mentioned low values related to the web browser, contributed to the weak final result of the Trace factor. The respondents often use the same passwords for multiple accounts and change their Internet passwords less frequently. These results are consistent with the results by Moallem's research findings of less frequent usage of complex passwords (Moallem, 2019) and the different awareness levels of passwords highlighted by Senthilkumar and Easwaramoorthy. (Senthilkumar & Easwaramoorthy, 2017)

Students in different disciplines pay different attention to certain factors; IT students are more careful in the case of Avoiding the untrusted, Precaution, and Leaving no trace factors, but less so in Protection of payment information. The responding law students prioritize the protection of their personal data, but in their case, for example, the area of Leaving no Trace is less emphasized. Technology students were lower than the other students in each field. The social students produced mixed results; in their case, Protecting privacy and Protection of payment was higher, but Precaution and Leaving no trace were even lower. All this leads to the conclusion that the respondent students in different fields require the development of different areas of awareness.

In an attempt to grasp the level of awareness regarding information security, the associated risks, and their overall impact, numerous research studies have been conducted. The results indicate that among the various participants, including educators, researchers, students, and employees, need to improve their essential knowledge and understanding of the importance of information security principles and their practical application in their daily responsibilities. (Al-Janabi & Al-Shourbaji, 2016; Moallem, 2019; Senthilkumar & Easwaramoorthy, 2017; Mai & Tick, 2021; Garba et al., 2020)

Various proposals for the development of awareness can be found in many papers dealing with security awareness. There are various gamification solutions for teaching many topics, such as the Unity role-playing application for the Android platform, which focuses on the security of passwords in Scholefield and Shepherd's study. (Scholefield & Shepherd, 2019) Similar attempt by the tabletop game Risk, which can help to enhance cyber security awareness among individuals in non-technical roles within organizations. It offers an interactive learning setting in which participants can develop their understanding of cyber security threats and protective measures. Players are immersed in the roles of both attackers and defenders of vital assets within a fictional organization, allowing them to build expertise in this domain. (Hart et.al., 2020)

While these solutions stand out, unfortunately, Cybersecurity Awareness Campaigns (CSAC) campaigns do not always reach their desired impact and may lead to failing to change people's behavior regarding security appropriately. (Bada et.al., 2019) Establishing an information security awareness program to reduce end-user errors in following security guidelines necessitates a systematic approach. (Siponen, 2000) Therefore, further awareness-related research would be necessary to find the appropriate effectiveness.

5. Conclusion

In conclusion, the respondents are more security conscious, but it's important to note the substantial contrast between the individual factors, items, and the study area of the participating students. The study reveals a diverse range of information security awareness levels among students from different disciplines. IT students tend to be more cautious about web browsing and password security, while law students prioritize personal data protection, and social science students show mixed results across various factors. Despite various educational efforts, including gamification and interactive learning tools, there remains a significant need for tailored awareness programs to effectively improve security practices across all fields. The research underscores the necessity for continued efforts and systematic approaches to enhance information security awareness and reduce end-user errors.

Bibliography

UNESCO (2021): Reimagining our Futures Together- a New Social Contract for Education. *Report from the International Commission on the Future of Education.* (2021) https://unesdoc.unesco.org/ark:/48223/pf0000379707 (2023.12.01.)

UNICEF (2020): Children at increased risk of harm online during global COVID-19 pandemic. https://www.unicef.org/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic (2023.12.01.)

Hinckley, S. D. (2002): Your Money or Your Speech: The Children's Internet Protection Act and the Congressional Assault on the First Amendment in Public Libraries. https://elibrary.law.psu.edu/fac_works/2/ (2023.11.23)

Ribble, M. (2015): *Digital Citizenship in Schools Nine Elements All Students Should Know.* International Society for Technology in Education, Washington DC.

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), 1-30.

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(2), 75–91.

Moallem, A. (2019): Cyber Security Awareness Among College Students. In Ahram, Tareq Z & D. Nicholson (Eds.): *Advances in Human Factors in Cybersecurity*. Springer International Publishing, 79-87.

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.

Scholefield, S., Shepherd, L. (2019): Gamification Techniques for Raising Cyber Security Awareness. *HCI for Cybersecurity, Privacy and Trust*. Springer International Publishing, 191-203.

Hart, S., Margheri, A., Paci, F., Sassone, V. (2020): Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*. Elsevier, 95.

Bada, M., Sasse, A., Nurse, J., (2019): Cyber Security Awareness Campaigns: Why do they fail to change behaviour? URL https://arxiv.org/abs/1901.02672 (2011.11.23.)

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.

Garba, A., Sirat, M.B., Hajar, S., Bukar I. (2020): Cyber Security Awareness Among University Students: A Case Study. *Science Proceeding Series*, 2(1), 82-86.

Siponen, M. (2000): A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41.

Authors

Gabriella Rosta, University of Pécs (Hungary), E-mail: rosta.gabriella@uni-nke.hu

László Bottyán, University of Pécs (Hungary), E-mail: laszlo@bottyan.com

László Bognár, University of Dunaújváros (Hungary), E-mail: bognarl@uniduna.hu