Gradus Vol 11, No 1 (2024)
ISSN 2064-8014

FEELING SAFE ONLINE AND EXPERIENCE WITH CYBER INCIDENTS AMONG UNIVERSITY STUDENTS

László Bottyán [0009-0008-4384-3856] [1*]

[1] Doctoral School of Education, University of Pécs, Hungary
https://doi.org/10.47833/2024.1.CSC.001

Keywords:
Cybersecurity
Security awareness
E-learning security
Online threats

Article history:
Received 5 November 2023
Revised 22 November 2023
Accepted 29 November 2023

Abstract
The field of education increasingly depends on technology to manage extensive volumes of information, underscoring the paramount importance of cybersecurity. Security breaches are rising within the education sector, necessitating the preemptive improvement of awareness. Within this article, we will delve into the findings of a survey that inquired with university students about their perceptions of safety in the digital realm and their encounters with cybersecurity events. The outcomes shed light on the fact that while a majority of students do perceive online safety, a noteworthy portion has already encountered security incidents.

1 Introduction

In the era of Industry 4.0 and globalisation, the pervasive influence of evolving information and communication technologies is evident in various domains. The rapid and far-reaching changes worldwide have a significant impact on education. [1] Of course, this rapid spread of technology also increases the amount of data and systems that need to be protected. There are many reports on data security incidents or current threats.

We highlight two examples. Risk Based Security (RBS), a US company specialising in data breach intelligence, publishes an annual report on publicly disclosed data breaches. Looking at the number of data breaches by sector, the education sector ranked seventh in 2021, with 328 reported breaches. [2] American multinational technology company Microsoft Inc.'s Global Threat Activity website shows the countries or regions with the most malware encounters in the last 30 days worldwide, based on 77,624,913 devices on the day of analysis. The real-time report shows that the most affected industry by reported enterprise malware encounters in the last 30 days is education, with 79.27%. [3]

These two examples show that the topic is current and essential.

2 International research on students' awareness of cybersecurity

Researchers Garba et al. conducted a survey to assess the awareness and enthusiasm of Nigerian university students towards cybersecurity. The survey aimed to determine the students' level of knowledge about cyber-attacks and how to mitigate them, as well as whether cybersecurity awareness programmes were included in university curricula. Initial results showed that students had a basic knowledge of cybersecurity but needed to become more familiar with ways to protect their data. Furthermore, most universities in Nigeria still need active cybersecurity awareness programmes to improve students' knowledge on how to protect themselves from cyber threats. [4]

Al-Janabi and Al-Shourbaji conducted a study on information security awareness among academic staff, researchers, students and employees in educational environments in the Middle East. The aim was to assess the level of understanding of information security, its associated risks and its overall impact on institutions. The results showed that the participants needed to gain

* Corresponding author. E-mail address: laszlo@bottyan.com

knowledge and understanding of information security principles through comprehensive awareness and training programmes. [5]

Moallem conducted a study in the Silicon Valley region of California, USA, with the aim of investigating students' awareness and attitudes towards cybersecurity. As the composition of students in Silicon Valley is very ethnically diverse, the study aimed to observe how much tech-savvy students are aware of cyber-attacks and how they protect themselves from such threats. Some of the interesting findings are that despite the high-tech and innovative environment, students need to be more aware of how to protect their data. Furthermore, educational institutions are not actively working to improve students' awareness of how to protect themselves from potential cyber-attacks such as identity theft and ransomware. [6]

A comparative study between university students in Hungary and Vietnam aimed to determine students' attitudes, awareness, and perceptions of personal privacy and cybersecurity of social media sites. Results showed that students lack fundamental knowledge of cybersecurity and good practices in their daily experiences regardless of their geographical location. [7]

Nagy et al. assessed users' cybersecurity awareness by categorising them based on their skills and awareness levels: naive, typical or aware; then assigning probabilities to each category to describe the likelihood of dangerous responses in the event of a cyberattack. The results show that even small differences in skill levels can have a significant impact on an organisation's cybersecurity posture. [8] Hadarics et al. highlighted in their study that user behaviors strongly influence the organization's vulnerability, and a mathematical model was also written for this. [9]

3 Method

The original questionnaire consisted of 30 statements. In this study, we will focus on the demographic statements and the last two cybersecurity statements, which are designed to assess respondents' overall sense of security in cyberspace and whether they have ever been the victim of an information security attack - for example, fraud, hacking, harassment, online abuse, or virus/ransomware attack.

The target population consisted of undergraduate students at the University of Dunaújváros and the University of Public Service in Hungary. Convenience sampling was used to recruit students from both universities, regardless of their level of education. The respondent university students come from different fields of study: law, social sciences, public service, IT and engineering.

Google Forms was used to collect the data, and IBM SPSS Statistics v25 and Minitab v21 software were used to analyse the data.

4 Results

A total of 106 students took part in the research, 48 males and 58 females. The average age of the respondents is 21 years. This study focuses on two statements: "I feel generally safe in cyberspace" and "I have been a victim of an information security incident (fraud, hacking, harassment, online abuse, virus/ransomware attack, etc.)".

For the first statement, the mean score is 2.80 on a 4-point Likert scale (1-Not at all; 2-Mostly no; 3-Mostly yes; 4-Yes, very much), indicating that respondents feel more secure in cyberspace than not. (*Table 1; Figure 1*) Regarding the second statement, the mean score is 1.45 on a 3-point Likert scale (1-Never; 2-Once or twice in my life; 3-Three or more times), indicating that almost half of the respondents have been victims of a cybersecurity incident. (*Table 1; Figure 2*)

Table 1. Descriptive statistics of the cybersecurity awareness questionnaire

	N	*Minimum*	*Maximum*	*Mean*	*Std. Deviation*
Age of the responder	106	17	34	21.00	3.071
I feel that I am generally safe in the cyberspace	106	1	4	2.80	0.576

I have been the victim of an information security incident (fraud, hacking, harassment, online abuse, virus / ransomware attack, etc.)	106	1	3	1.45	0.571
Valid N (listwise)	106				

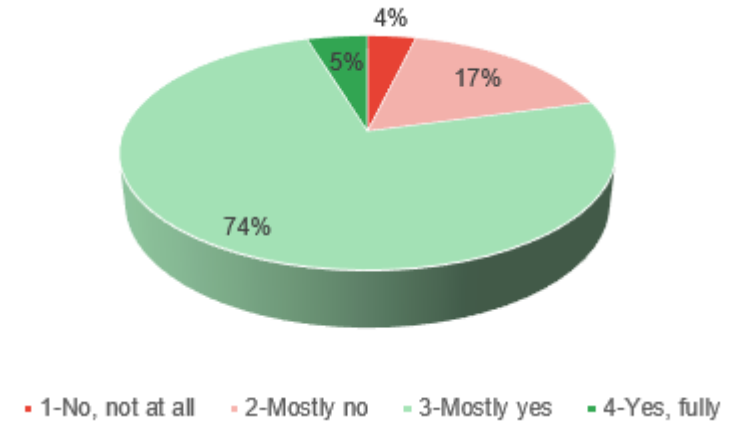

Figure 1. Distribution of responses – I feel that I am generally safe in the cyberspace

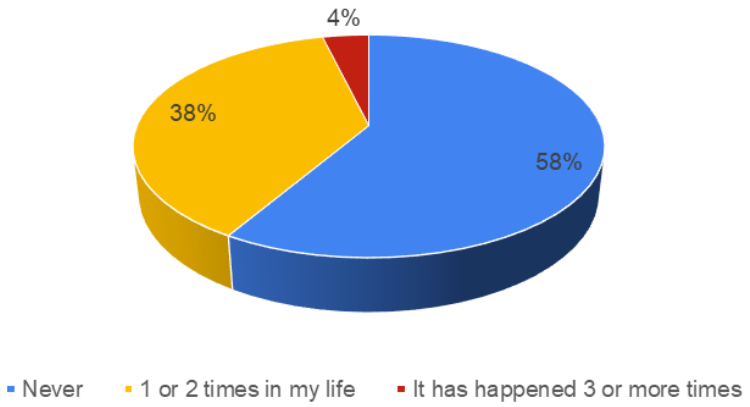

Figure 2. Distribution of responses – I have been the victim of an information security incident

Looking at the gender distribution of the statement "I feel generally safe in cyberspace", female respondents feel slightly safer in cyberspace than male respondents. (*Table 2; Figure 3*)

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

	1-No, not at all	*2-Mostly no*	*3-Mostly yes*	*4-Yes, fully*	*All*
Female	3	10	45	0	58
	2.189	9.849	43.226	2.736	
Male	1	8	34	5	48
	1.811	8.151	35.774	2.264	
All	4	18	79	5	106

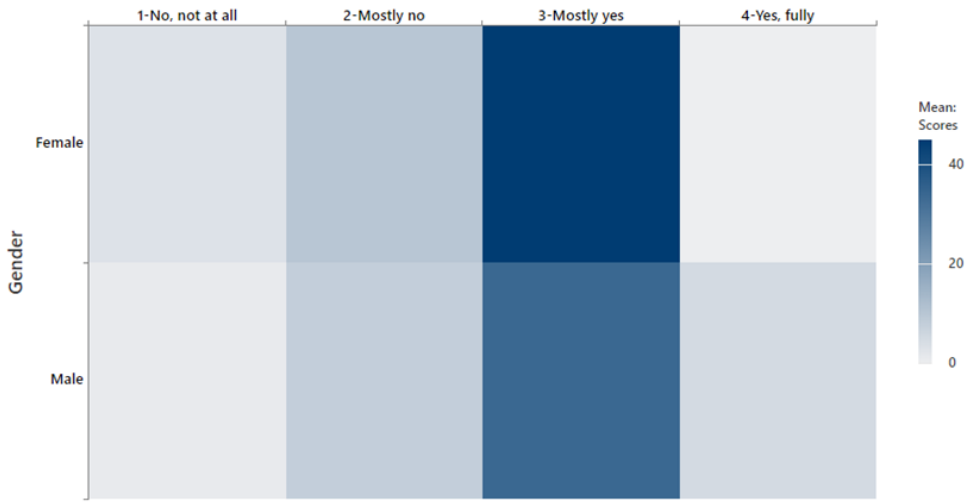

Figure 3. Heatmap - I feel that I am generally safe in the cyberspace

An independence test was carried out with a Chi-square test, where the P-value < 0.05 means that the level of feeling safe and the gender of the respondent are not independent of each other. (*Table 3*)

Table 3. Chi-Square test – I feel that I am generally safe in the cyberspace

	Chi-Square	*DF*	*P-Value*
Pearson	6.872	3	0.076
Likelihood Ratio	8.792	3	0.032

If we check the gender distribution of the statement "I have been a victim of an information security incident" and group them into no or yes answers, regardless of how many times it has happened, the results show that it is less likely to happen with the younger respondents. (*Table 4; Figure 4*)

Table 4. Tabulated statistics - I have been the victim of an information security incident

	Never	*Yes, it happened*	*All*
<=20	40	20	60
	35.09	24.91	
> 20	22	24	46
	26.91	19.09	
All	62	44	106

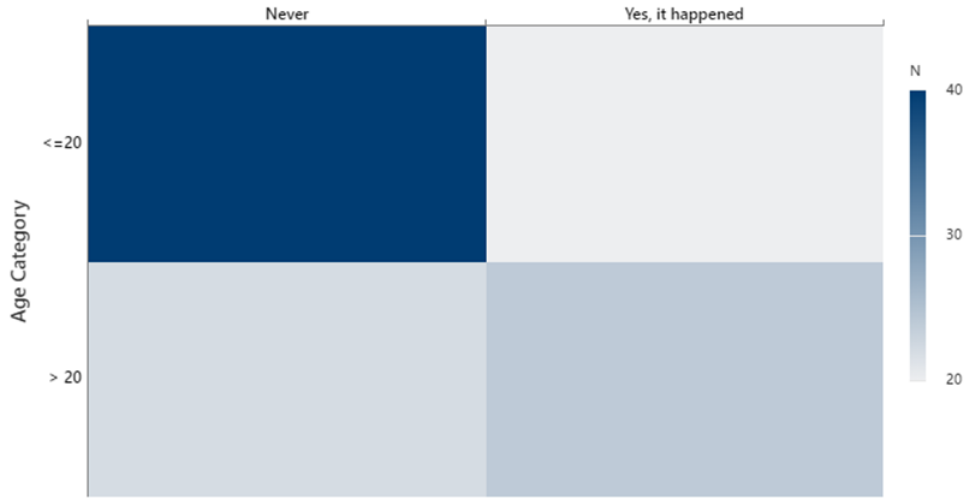

Figure 4. Heatmap - I have been the victim of an information security incident

An independence test was carried out using a chi-squared test with a P-value of 0.051, which means that being a victim of an incident is not independent from the age (*Table 5*).

Table 5. Chi-Square test – I have been the victim of an information security incident

	Chi-Square	*DF*	*P-Value*
Pearson	3.807	1	0.051
Likelihood Ratio	3.811	1	0.051

Conclusion

This research sought to answer the question of how safe groups of students at two universities feel in cyberspace and whether they have ever been victims of an information security incident. It was concluded that the majority of respondents felt safe and that the level of feeling and the gender of the respondents were not independent of each other. It was also concluded that almost half of the respondents had been victims of an information security incident, which is not independent of the age of the students who responded.

Awareness of potential security threats is essential to prepare for and protect against them. Educating students and teachers about security best practices and the importance of security is critical to creating a strong security culture within educational institutions. By doing so, educational organisations can significantly improve their overall security posture.

References

[1] Balyer, A., & Öz, Ö.: Academicians' Views on Digital Transformation in Education. International Online Journal of Education and Teaching, 2018, Vol. 5 No.4, pp 809–830. https://eric.ed.gov/?id=EJ1250526

[2] Risk Based Security Inc. 2021 Year End Report - Data Breach QuickView, 2022. https://pages.riskbasedsecurity.com/2021-year-end-data-breach-report

[3] Microsoft. Cyberthreats, viruses, and malware - Microsoft Security Intelligence, 2019. https://www.microsoft.com/en-us/wdsi/threats

[4] Garba, A., Maheyzah B. S., Siti H., Ibrahim B. D.: Cyber Security Awareness Among University Students: A Case Study. Science Proceedings Series, 2020, Vol. 2, No. 1, pp 82–86. DOI: doi.org/10.31580/sps.v2i1.1320

[5] Al-Janabi, S., & Al-Shourbaji, I.: A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information & Knowledge Management, 2016, Vol. 15, No 1, 1650007. DOI: doi.org/10.1142/s0219649216500076

[6] Moallem, A.: Cyber Security Awareness Among College Students. Advances in Intelligent Systems and Computing, 2018, pp 79–87. DOI: doi.org/10.1007/978-3-319-94782-2_8

[7] Mai, P. T., & Tick, A.: Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. Acta Polytechnica Hungarica, 2021, Vol. 18, No. 8, pp 67–89. DOI: doi.org/10.12700/aph.18.8.2021.8.4
[8] Bognár, L., Jóos, A., & Nagy, B.: An improvement for a mathematical model for distributed vulnerability assessment. Acta Universitatis Sapientiae, Mathematica, 2018, Vol. 10, No. 2, pp 203–217. DOI: doi.org/10.2478/ausm-2018-0017
[9] Hadarics, K., Győrffy, K., Nagy, B., Bognár, L., Arrott, A., Leitold, F.: Mathematical Model of Distributed Vulnerability Assessment, Proceedings of Conference SPI 2017: Security and Protection of Information, 2017, pp. 45-57.