Cybersecurity Awareness and Ransomware-Related Practices among University Students

Laszlo Bottyan [1*], Balint Nagy [2]

1 Self-employed, Budapest, Hungary, laszlo@bottyan.com*

2 University of Dunaujvaros, Dunaujvaros, Hungary, Óbuda University, Kandó Kálmán Faculty of Electrical Engineering, Budapest, Hungary, nagyb@uniduna.hu

Abstract

The education sector is now one of the most targeted domains of cyberattacks, with ransomware being the most prevalent threat. The present study focuses on university students' security behaviours related to ransomware, especially email and phishing vulnerability, user access and credential practices, system and software hygiene, data protection habit, and threat perception. The sample was taken in a Hungarian university with a sample size of 85 respondents. The measuring instrument was an online questionnaire consisting of 11 questions answered on a 3-point Likert scale. The results present a mixed picture: respondents appear more security-aware in relation to e-mail phishing risks and system and software security hygiene, while showing lower levels of security in user access, credential practices, data backup, and threat perception. The analysis is descriptive and exploratory, relying on item-level proportions. The study provides exploratory insights into student cybersecurity awareness, grounded in data from a single higher education institution, and highlights directions for future, broader investigations. Targeted awareness campaigns with the mentioned focus points are required to support a more comprehensive defence against ransomware.

Keywords: higher education, cyber hygiene, information security behaviour, ransomware awareness

1. Introduction

Today's education sector heavily uses information and communication technologies during teaching and learning. Learning management systems, virtual classes, and e-learning applications make it more accessible and engaging. However, the significant use of digital technology also involves the challenge of maintaining cybersecurity in this modern learning environment. As digitalization is becoming more prevalent in educational institutions, their cybersecurity threats are expected to increase. Institutions handle sensitive personal data, from logins and passwords used on various portals to financial data and even research-related data. Given that educational institutions are likely not spending as much on cybersecurity as industrial players, the data they handle is also at greater risk. However, research and daily news often point out that the human factor is the weakest link. The above shows why cybersecurity awareness among various educational stakeholders is such an important issue.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) define cybersecurity as "protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" (Cybersecurity and Infrastructure Security Agency, 2021). In the literature, it is often visualized as the C-I-A triad. According to the European Union Agency for Cybersecurity (ENISA) Threat Landscape 2024 report, ransomware is one of the prime threats in today's cyber environment. Ransomware is a type of cyberattack in which malicious actors take control of a target's assets and demand a ransom to restore their availability or prevent the public exposure of the target's data (ENISA, 2024). Ransomware mainly jeopardizes confidentiality and availability, two parts of the C-I-A triad. Once triggered, users experience availability loss because they can no longer access their data.

Recent trends indicate that the education sector is becoming more vulnerable to cyber threats. In the first quarter of 2023, the Education and Research sector experienced the most significant impact, suffering the highest number of cyberattacks with an average of 2,507 per organization weekly. This marked a 15% increase compared to the first quarter of 2022. Many institutions in this sector faced challenges securing their extended networks and access points as they adapted to remote learning. In the meantime, this sector was the third most affected by ransomware (CheckPoint, 2023). According to the Phishing Activity Trends Report 3rd Quarter 2022 by the Anti-Phishing Working Group, 5% of all ransomware attacks are directed at the education sector (APWG 2022). A Comparitech article details the rising number of ransomware attacks on educational institutions from 2018 to 2023, highlighting significant downtime costs—estimated at $53 billion globally—and disruptions to student learning. Schools and colleges, particularly in 2023, have seen a surge in attacks, with ransom demands averaging $1.5 million. The analysis shows that colleges suffer higher record breaches and downtime than schools despite schools facing higher ransom demands (Moody, 2023). Verizon's 2022 Data Breach Report (DBIR) highlights an increase in ransomware attacks, accounting for over 30% of education sector breaches driven by limited resources and large volumes of sensitive student data. Attackers often use "double" and "triple extortion" methods, targeting school systems and parents (Verizon, 2022). The DBIR report also points out that most security breaches in the education sector, around 90%, are caused by system intrusions, social engineering, and human error. Higher education institutions often face data breaches due to their valuable research and personal data, and they have unique vulnerabilities due to their open, collaborative culture (Ulven and Wangen, 2021). Further education or higher education institutions are more likely to experience various attack types, such as viruses, malware, and unauthorized access to data or networks (UK Department for Science, Innovation & Technology, 2024).

2. Literature review

Ulven and Wangen explore cybersecurity threats within universities in their research, which often face data breaches due to the valuable research and personal data they hold. The study categorizes the risks into assets, threat events, threat actors, and vulnerabilities, highlighting frequent threats like hacking, malware, and social engineering (Ulven and Wangen, 2021). Khalid et al. examined the level of cybersecurity awareness among university students in Malaysia. The study used a questionnaire to measure the respondents' awareness across areas like cyberbullying, personal information protection, cybersex, internet banking, internet addiction, and self-protection. The sample consisted of 142 second-year education students. The results showed that while the respondents displayed a high level of awareness regarding certain aspects of cyber security, such as cyberbullying, personal information, and internet banking, they had less knowledge about cybersex and self-protection (Khalid et al., 2018). Alqahtani examined cybersecurity knowledge among university students in Saudi Arabia based on 450 responses. Findings reveal that social media behaviours most significantly impact awareness, followed by browser and password security knowledge. Although students recognize the importance of cybersecurity, they need to improve their practical application of secure behaviours (Alqahtani, 2022). Gabra et al. researched Nigerian Universities to assess students' cybersecurity awareness levels. Among the questions about using hard-to-guess passwords, 204 answered no from 367; regarding opening an email from an unfamiliar person, 219 said yes out of 367. This result indicates the respondents' lack of knowledge about phishing and password management (Gabra et al., 2020). Moallem's study aimed to assess students' cybersecurity awareness and attitudes in a very technocratic area of Silicon Valley in California, USA. With respect to the question measuring participants' cybersecurity knowledge, only 26% of the 247 surveyed agreed they were knowledgeable. Trust in the security of the university system varies; 57% consider it relatively secure, but 21% believe it is not safe. Regarding password management, 52% of respondents use two-factor authentication for some accounts, 24% use it for all accounts, 3% don't, and 8% do not know what it is (Moallem, 2019). Another study among Hungarian university students found that most respondents still do not implement secure password management in practice (Kollár & Katona, 2024). Further, diverse research is underway on the topic and examines numerous factors (Tick & Mai, 2024; Avci & Koca 2023). Chasanah and Candiwan examined Indonesian college students' cybersecurity awareness across attitudes, knowledge, and behaviour. They found that while overall awareness was rated "good" (around 80%), gaps remained in specific areas such as password management (Chasanah and Candiwan, 2025). Verma and Pawar investigated college students' cybersecurity awareness as active internet users, focusing on phishing, malware, and ransomware. Their findings show that while students demonstrate awareness of these threats, such awareness does not consistently translate into effective protective practices (Verma and Pawar, 2025). Wash, Rader, Mandia, and Fossen examined how users select passwords and found that password reuse remains widespread even when individuals are aware of the risks (Wash et al., 2017). Mathews and Haque investigated the risks of password reuse across websites of varying importance. They found that users often apply the same or similar passwords to multiple accounts, which creates cascading vulnerabilities—for example, a breach of a low-value account can endanger higher-value ones (Mathews and Haque, 2024). Marcatto, Mistichelli, and Ferrante explored how people perceive digital threats, showing that optimism bias is common and that AI is viewed as particularly unfamiliar and uncertain. This highlights how perceptions of severity and novelty shape cybersecurity awareness (Marcatto et al., 2025).

There are several ways to defend against ransomware attacks. Mohurle and Patil highlight that timely patch management and strong, unique passwords are critical first-line defences. They also stress the importance of offline backups to restore encrypted data without paying ransom (Mohurle & Patil, 2017). ENISA focuses on simple, cost-effective measures: isolate critical assets, restrict user rights, and perform routine backup and restore drills to ensure data availability (ENISA, 2020).

Overall, effective ransomware defence relies on a combination of regularly tested backups, consistent patching and software updates, robust endpoint protection, and the careful management of access rights through the enforcement of least-privilege controls.

3. Research questions and hypotheses

The purpose of this research is to conduct an exploratory analysis regarding the awareness levels of university students regarding cyber security by looking at self-reported behaviour, primarily seeking to uncover risk factors and misconceptions that are most prevalent. This research should help to establish some guidelines on how one could improve awareness regarding cyber security while providing a foundation for future, more in-depth research.

The study is guided by three central research questions:

- RQ1: To what extent are students aware of the most common cyber threats, such as phishing, ransomware, and other online attacks?

- RQ2: To what degree do students apply secure IT practices, including password management, account usage, system and antivirus updates, as well as backup and encryption routines?

- RQ3: How do students perceive the risks posed by cyber threats, and to what extent do they recognize that such threats affect individual users as well as large institutions or data-holding organizations?

Correspondingly, we formulated three hypotheses:

- H1: Most students are able to recognize the most common cyber threats, including phishing and ransomware attacks.

- H2: Students' security practices do not consistently reflect their awareness; password reuse, shared account usage, and insufficient application of backup or encryption remain widespread.

- H3: A proportion of students underestimate the risks of cyber threats at the individual level, if attacks primarily target large institutions or organizations.

4. Methods

To address these questions, undergraduate students were surveyed from four faculties (Engineering, Economics, Pedagogy, and Other) at the University of Dunaújváros using an 11-item cybersecurity behaviour questionnaire. Data were collected online during the autumn semester of 2024/2025. Demographic variables included gender, year of study, and field of study. Responses were measured on a three-point Likert scale, assessing students perceived knowledge of phishing and email security risks, risky internet use, attention to system settings, commitment to data protection, and password/account management practices.

Initial reliability analysis of the full 11-item scale yielded Cronbach's $\alpha = 0.699$. According to Nunnally (1978), "in early stages of research, reliabilities of 0.60 or higher are acceptable" (p. 226). Since our scale approaches the conventional 0.70 threshold, we consider its internal consistency adequate for this exploratory study. Ethical considerations were carefully observed: participation was voluntary, no personal data were collected, and respondents were informed of the study's purpose and their right to withdraw at any time.

The exploratory design was not intended to establish causal relationships but rather to provide a descriptive snapshot of students' cybersecurity awareness. Descriptive statistics were applied to identify patterns and highlight areas of vulnerability. The findings reveal gaps between awareness and practice, as well as misconceptions regarding the scope of cyber threats. These insights are valuable for universities seeking to design targeted training programs or regulatory improvements.

Beyond practical implications, the study contributes theoretically by structuring dimensions of cybersecurity awareness—online behaviour and risk perception, technical protection and system practices, and password management and threat awareness. This framework supports the identification of constructs for future research and enables comparative analyses across institutions.

In conclusion, this research offers a timely perspective on the cybersecurity culture of higher education. By mapping students' awareness, practices, and perceptions, the study provides baseline data for the development of institutional IT strategies and contributes to strengthening the cybersecurity culture of universities in an increasingly dynamic digital environment.

5. Results

5.1. Results of the individual risk behaviours

The sample comprised 85 respondents. Responses to eleven security-related items are reported as counts and percentages for three categories: Yes, I agree, I can't decide, and No, I don't agree. Table 1 presents the distribution of survey responses for each questionnaire item (Q1–Q11), showing counts and row percentages for each response category. It summarizes how respondents agreed, disagreed, or were undecided on each security- behaviour related statement.

5.2. Highlights of the item-level results towards positive security behaviour

In this section, we highlight some results that show highly positive cybersecurity behaviours from the respondents.

The responses to Question 6 clearly reveal the students' security-aware attitude. The trend suggests that a significant proportion of students recognize the crucial role of regular updates in defending against cyberattacks, see Fig. 1.

The data presented in Fig. 2 are concerning from a cybersecurity perspective, as phishing attacks aimed at obtaining user credentials remain among the most common forms of cyberattacks.

Table 1. Summary of responses per question

			Yes, I agree	I can't decide	No, I don't agree	TOTAL
Question - survey item	Q1: Attachments or links received in an e-mail from an unknown sender can be safely opened unless they are in the spam folder.	Count	23	6	56	85
		% within Question - survey item	27.1%	7.1%	65.9%	100.0%
	Q2: Emails asking for my username and password are not suspicious to me	Count	14	4	67	85
		% within Question - survey item	16.5%	4.7%	78.8%	100.0%
	Q3: I will download any file from the internet if I have an urgent need.	Count	20	10	55	85
		% within Question - survey item	23.5%	11.8%	64.7%	100.0%
	Q4: I'd rather download cracked software than buy it at full price because it's free.	Count	20	17	48	85
		% within Question - survey item	23.5%	20.0%	56.5%	100.0%
	Q5: Pop-ups are enabled in my browser because that's the only way most websites provide the full user experience.	Count	22	8	55	85
		% within Question - survey item	25.9%	9.4%	64.7%	100.0%
	Q6: I prefer to turn off automatic system and antivirus updates because they slow down my computer.	Count	12	5	68	85
		% within Question - survey item	14.1%	5.9%	80.0%	100.0%
	Q7: By encrypting the entire hard drive, I don't need to back up my files and data regularly.	Count	14	26	45	85
		% within Question - survey item	16.5%	30.6%	52.9%	100.0%
	Q8: I use the same account on my computer for daily activities like installing new software.	Count	53	15	17	85
		% within Question - survey item	62.4%	17.6%	20.0%	100.0%
	Q9: I use the same password for several Internet accounts, so I'm sure I will remember it.	Count	38	5	42	85
		% within Question - survey item	44.7%	5.9%	49.4%	100.0%
	Q10: Shorter passwords with capital letters and special characters are more secure than long passwords without a mix of these characters.	Count	39	10	36	85
		% within Question - survey item	45.9%	11.8%	42.4%	100.0%
	Q11: Ransomware attacks mainly target those who handle and store large amounts of personal or confidential data.	Count	40	22	23	85
		% within Question - survey item	47.1%	25.9%	27.1%	100.0%

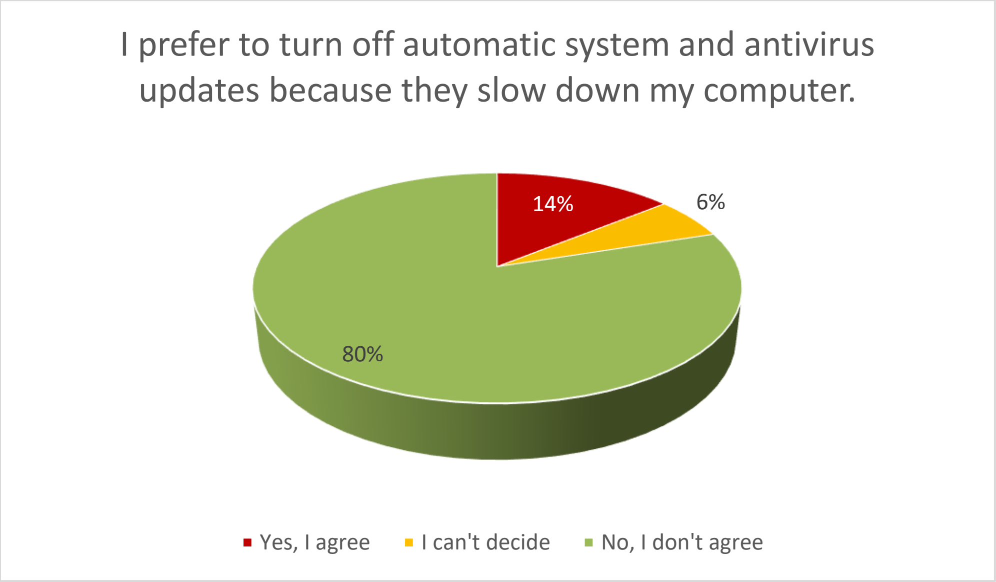

Fig. 1. Distribution of the answers in % on the statement " I prefer to turn off automatic system and antivirus updates because they slow down my computer" (Q6)".

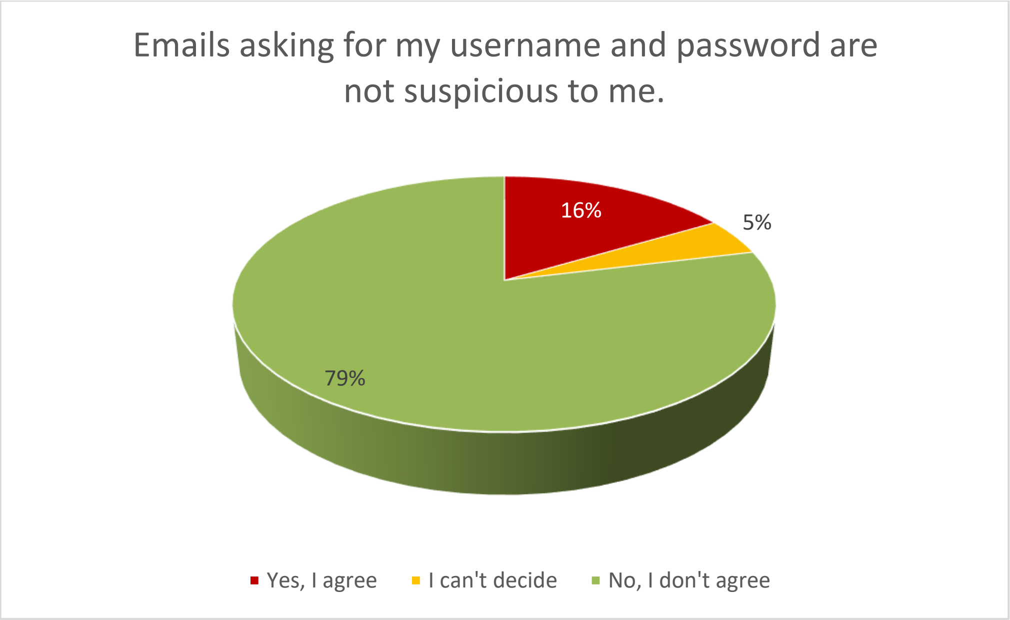

Fig. 2. Distribution of the answers in % on the statement "E-mails asking for my username and password are not suspicious to me." (Q2)

5.3. *Highlights of the item-level results towards less cautious security behaviour*

In this section, we present results indicating that respondents exhibit less cautious cybersecurity behaviours. The results suggest that most respondents are not fully aware of the importance of the principle of least privilege, a fundamental security concept in preventing cyberattacks. or Question 8, nearly two-thirds of the students—53 respondents—answered “yes” to using the same account for everyday activities and system-level tasks, while 15 were undecided, and 17 rejected this practice, see Fig. 3.

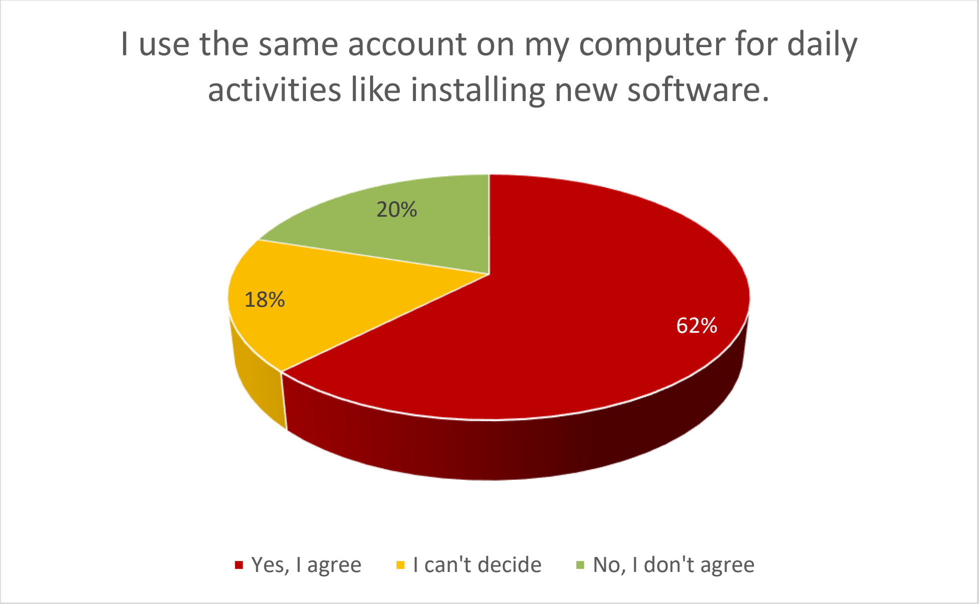

Fig. 3. Distribution of the answers in % on the statement " I use the same account on my computer for daily activities like installing new software." (Q8)

Nearly half of the respondents (44.7%) reported using the same password across multiple platforms, 5.9% were uncertain, while 49.4% indicated that they avoid this practice, see Fig. 4.

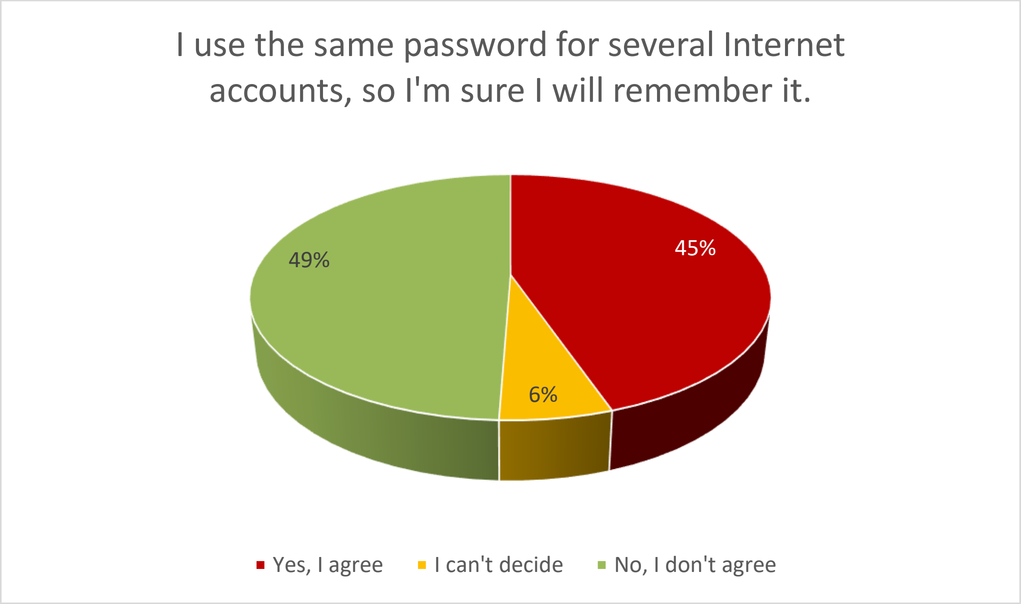

Fig. 4. Distribution of the answers in % on the statement " I use the same password for several Internet accounts, so I'm sure I will remember it." (Q9)

For Question 7, 16.5% of students agreed that encryption alone makes backups unnecessary, 30.6% were undecided, while 52.9% rejected this claim, see Fig. 5. These results reveal that nearly one-third of respondents are not fully aware of the distinct roles of encryption and backup in data protection.

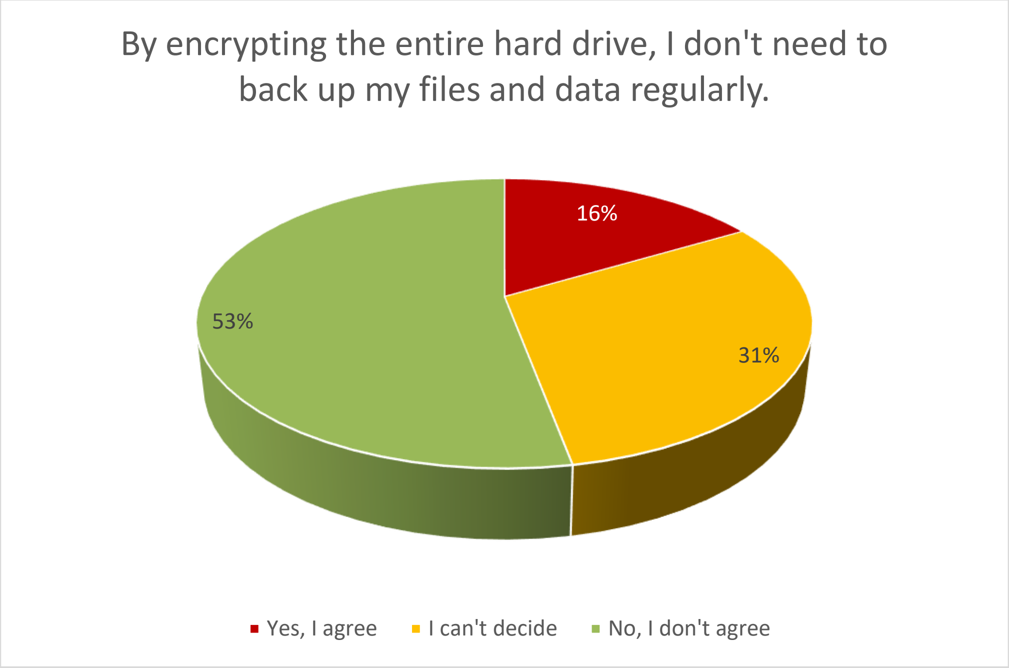

Fig. 5. Distribution of the answers in % on the statement "By encrypting the entire hard drive, I don't need to back up my files and data regularly." (Q7)

For Question 11, nearly half of the students (47.1%) agreed that ransomware mainly targets institutions handling large amounts of data, 25.9% were uncertain, and 27.1% disagreed, see Fig. 6.

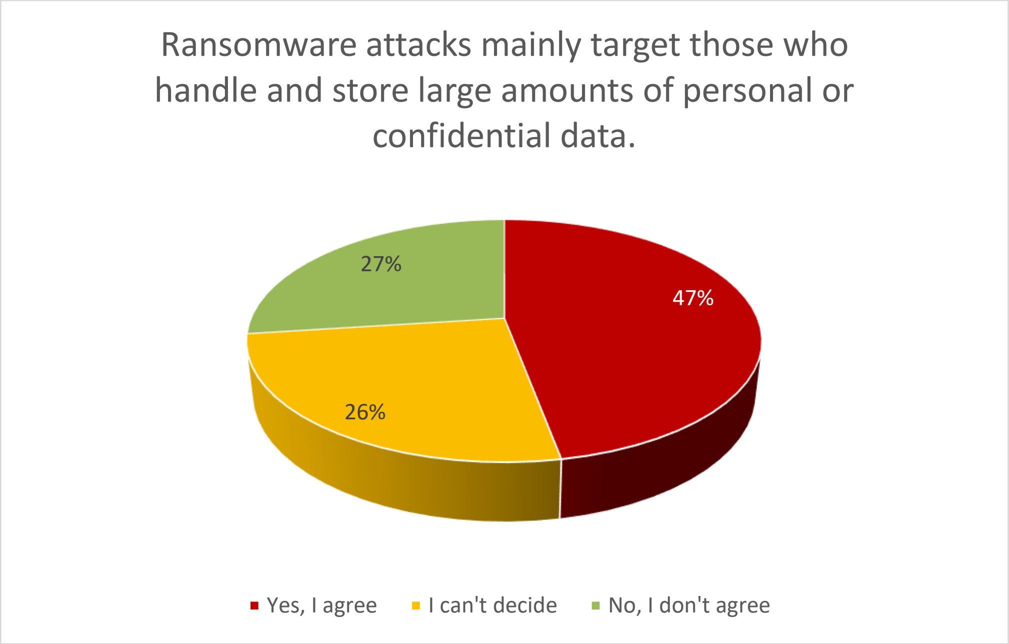

Fig. 6. Distribution of the answers in % on the statement "Ransomware attacks mainly target those who handle and store large amounts of personal or confidential data." (Q11)

The results indicate that most students are aware of the most common cyber threats, such as phishing and the importance of regular system updates. At the same time, several areas of uncertainty and misconception can be observed, including password reuse, the role of encryption, and the identification of ransomware targets. This suggests that while students are generally security-conscious, the depth of their awareness varies, and there remains a need for practice-oriented development of cybersecurity knowledge. Overall, the data clearly highlight the domains in which education should be strengthened to enhance both personal and institutional security.

5.4. Inferential Analyses of Less Cautious Security Behaviour

In this section, we selected Q7, Q8, Q9, and Q11 because they represented the weakest items in the survey. The chi-square analyses revealed no statistically significant differences across faculties (all p-values > 0.05), indicating that these problems are general among students regardless of their field of study.

Table 2. Chi-Square Test Results for Less Cautious Security Behaviors

Question (item)	Pearson χ^2	df	p-value
Q7 - By encrypting the entire hard drive, I don't need to back up my files and data regularly.	7.6	6	0.27
Q8 - I use the same account on my computer for daily activities like installing new software.	9.95	6	0.127
Q9 - I use the same password for several Internet accounts, so I'm sure I will remember it.	6.2	6	0.4
Q11 - Ransomware attacks mainly target those who handle and store large amounts of personal or confidential data.	9.33	6	0.156

6. Discussion

Both Chasanah and Candiwan (2025) and Verma and Pawar (2025) highlight that college students generally demonstrate a relatively high level of cybersecurity awareness, particularly in recognizing threats such as phishing, yet notable gaps remain in specific practices, such as password management or translating awareness into effective protective behaviour. These results reinforce Hypothesis H1, confirming that recognition of threats is common but not uniformly extended to all types of risks, nor consistently reflected in secure practices. The results of this research, such as the 78.8% phishing recognition rate, fit within this broader pattern, underscoring that awareness is necessary but insufficient without corresponding behavioural safeguards. This result underscores the continued importance of strengthening digital self-defence and cybersecurity education within higher education environments.

System update practices also reflect positive awareness: most students did not disable automatic updates, which is a fundamental element of cyber hygiene in higher education environments. Such an attitude not only enhances individual device security but also contributes to safeguarding the institution's IT infrastructure. Conscious update management is a fundamental element of cybersecurity culture, and its presence is a prerequisite for a secure digital learning environment.

Password practices have been widely studied, and the evidence consistently highlights a gap between users' awareness of risks and their actual behaviour. Wash et al. (2017) showed that password reuse remains prevalent even when individuals acknowledge its dangers, reflecting the tension between usability and security. Building on this, Mathews and Haque (2024) demonstrated that users often apply the same password across websites of differing importance, thereby creating cascading vulnerabilities in which a breach of a low-value account can compromise more critical ones. Together, these studies reinforce Hypothesis H2, which posits that awareness of security risks does not necessarily translate into secure practices. The results, such as the 44.7% of students who reuse passwords across accounts, align closely with this body of research, situating the results within a broader pattern of risky password habits. This can lead not only to unauthorized access to personal data but also to identity theft and broader security incidents. This question therefore serves as an important indicator of the extent to which students consciously manage their digital identities.

Account handling practices also reveal gaps: nearly two-thirds of students reported using the same account for everyday activities and system-level tasks, indicating limited awareness of the principle of least privilege. This behaviour increases potential damage in case of compromise and highlights the need for targeted awareness campaigns. This question is particularly important because it does not merely address a technical habit but serves as a key indicator of user awareness and system-level security mindset. The findings highlight that strengthening cybersecurity knowledge remains a priority for both IT and non-IT students alike.

Data protection misconceptions were also evident. About one-third of students believed or were uncertain that encryption alone substitutes for backups. This reflects a misunderstanding of layered security, where encryption protects confidentiality but does not ensure availability against ransomware or hardware failure. Clarifying this distinction is essential in training programs.

Data security is a multi-layered system in which encryption represents only one level of defence. The fact that about one-third of students remain uncertain on this issue indicates that the importance and function of backups must be further emphasized in training programs aimed at improving IT awareness.

Marcatto, Mistichelli, and Ferrante (2025) provide strong support for Hypothesis H3, which argues that individual users do not always perceive their own cyber risk. Their psychometric study shows that optimism bias leads many people to assume they are less vulnerable than others, while the “unknown risk” dimension makes emerging threats - such as AI - feel distant or unfamiliar. This combination results in underestimating personal exposure and framing cyberattacks as problems for institutions or “others.” The finding of this study that 27–30% of respondents in Q11 were uncertain or failed to recognize personal risk reflects the same mechanisms identified in their research, situating these results within a broader pattern of distorted risk perception. This question uncovers a specific misconception and underscores the importance of emphasizing in cybersecurity education that digital threats do not affect only ‘big players,’ but everyone who uses devices, data, or online services.

The analysis of the survey data reveals a nuanced picture of university students’ cybersecurity awareness and behaviour. Most participants demonstrated competence in identifying phishing emails, providing partial support for Hypothesis H1, yet considerable uncertainty emerged in recognizing ransomware attacks and the risks faced by individual users. Hypothesis H2, which addressed the gap between security practices and awareness, was also substantiated: while students generally maintain appropriate practices regarding system and antivirus updates, many reported reusing the same password across multiple accounts and relying on a single user account for everyday activities. Finally, Hypothesis H3—that a proportion of students underestimate the personal risks associated with cyber threats—was confirmed, as nearly one-third did not acknowledge that attacks may target individuals as well as large institutions.

Taken together, these findings indicate that students possess a baseline level of cybersecurity awareness, yet certain aspects of practice and risk perception remain underdeveloped and warrant further attention. The survey highlights the complexity of students’ cybersecurity behaviour, with notable vulnerabilities emerging in their responses to ransomware. Accordingly, the study addresses three principal dimensions: awareness of prevalent cyber threats; the security practices embedded in everyday computer use, including password management, account handling, and system updating; and the perception of risks posed by cyber threats, particularly the recognition that such risks extend to individual users as well as institutions.

The results underscore critical areas where further education and awareness campaigns are indispensable—for example, reducing administrative-account reuse through least-privilege guidance, promoting unique long passwords and password managers to curb reuse, and clarifying that encryption is not a substitute for backups and that ransomware can be opportunistic. Beyond these practical implications, the study contributes theoretically by structuring dimensions of cybersecurity awareness, thereby supporting the identification of constructs for future research and enabling comparative analyses across institutions.

At the same time, several limitations must be acknowledged: the study is based on a small, voluntary sample from a single institution, relies on self-reported data, and adopts a cross-sectional design, which precludes generalization, causal inference, or the assessment of temporal change. Nevertheless, the exploratory nature of the research provides a solid foundation for larger, multi-institutional studies. Future work will aim to collect behaviour-based, objective data through system-usage logs and phishing simulations, to design targeted training interventions addressing identified knowledge gaps and risky practices, and to evaluate their impact using controlled group methods. Given the rapidly evolving nature of cyber threats, periodic reassessments are planned to monitor the progression of students' awareness and their adaptation to emerging risks.

7. Conclusion

The findings of this study yield several practically relevant insights. While most students are able to recognize fundamental forms of cyber threats, such as phishing and malicious emails, this awareness does not consistently translate into adequate protection or sustainable security practices. This underscores that cybersecurity education must extend beyond the transmission of knowledge to include the shaping of behavioural habits.

For practice, this highlights the need for further awareness-raising and skill-development programs that simulate real decision-making contexts, such as password management, system updating, and responses to data security incidents. The results confirm that cognitive knowledge alone is insufficient; fostering sustainable cybersecurity behaviour requires targeted educational interventions. At the institutional level, strengthening regulatory and technical support may also be warranted, including automatic security updates, encouragement of password manager use, and mandatory two-factor authentication. Within educational environments, regular interactive training and simulations—such as phishing exercises—can further enhance students' security maturity. Overall, the study emphasizes that preparing students for cybersecurity cannot end with information transfer but must involve continuous, practice-oriented development that addresses attitudes, motivations, and behaviours.

Future research should extend these findings into experimental settings, for example by employing realistic but safe phishing simulations to examine actual behaviour. Additional studies could evaluate the effectiveness of educational interventions designed to enhance cybersecurity awareness, comparing different methodological approaches. Expanding the sample to include students from multiple institutions would improve generalizability, while exploring demographic and psychological factors—such as risk aversion or digital self-efficacy—could shed light on the drivers of security aware behaviour. Ultimately, future work should aim to integrate cognitive and behavioural dimensions of cybersecurity awareness to establish a stronger foundation for effective educational strategies.

8. References

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. Applied Sciences, 12(5), 2589. https://doi.org/10.3390/app12052589

Anti-Phishing Working Group. (2022, December 12). Phishing activity trends report: 3rd quarter 2022. https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

Avci, İ., & Koca, M. (2023). Cybersecurity attack detection model using machine learning techniques. Acta Polytechnica Hungarica, 20(7), 29–44. https://doi.org/10.12700/APH.20.7.2023.7.2

Bottyan, L. (2025). Egyetemi hallgatók internetes fiók- és jelszókezelési szokásai. Dunakavics, 13(1), 41–53.

Check Point Software Technologies Ltd. (2023). 2023 cyber security report. https://resources.checkpoint.com/report/2023-check-point-cyber-security-report

Cybersecurity and Infrastructure Security Agency. (2021, February 1). What is cybersecurity? https://www.cisa.gov/news-events/news/what-cybersecurity

ENISA European Cybersecurity Agency. (2020). ENISA threat landscape 2020: Ransomware. https://www.enisa.europa.eu/publications/ransomware

Gabra, A., Sirat, M., Hajar, S., & Dauda, I. (2020). Cyber security awareness among university students: A case study. Science Proceedings Series, 2(1), 82–86. https://readersinsight.net/SPS/article/view/1320

Khalid, F., Daud, M. Y., Mohd Jasmy, Rahman, A., Khalid, M., & Nasir, M. (2018). An investigation of university students' awareness on cyber security. International Journal of Academic Research in Business and Social Sciences, 8(9), 1–12.* https://api.semanticscholar.org/CorpusID:250960643

Kollar, A. M., & Katona, J. (2024). Enhancing password security: Analyzing password management practices among IT students. In 2024 IEEE 7th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE) (pp. 59–64). IEEE. https://doi.org/10.1109/cando-epe65072.2024.10772755

Lella, I., Theocharidou, M., Magonara, E., Malatras, A., Naydenov, R., Ciobanu, C., Chatzichristos, G., Ardagna, C., Corbiaux, S., & Van Impe, K. (2024). ENISA threat landscape 2024. ENISA. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

Moallem, A. (2019). Cyber security awareness among college students. In T. Z. Ahram & D. Nicholson (Eds.), Advances in human factors in cybersecurity (pp. 79–87). Springer. https://doi.org/10.1007/978-3-319-94782-2_8

Moody, R. (2023, September 15). Ransomware attacks on schools and colleges around the world. Comparitech. https://www.comparitech.com/blog/vpn-privacy/school-ransomware-attacks-worldwide/

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5), 1938–1940. https://doi.org/10.26483/ijarcs.v8i5.4021

Tick, A., & Mai, P. (2024). Cyber security awareness and the behaviours of higher education students using smartphones in Vietnam. Acta Polytechnica Hungarica, 21(12), 111–131. https://doi.org/10.12700/APH.21.12.2024.12.7

UK Department for Science, Innovation & Technology. (2024, April 9). Cyber security breaches survey 2024: Education institutions annex. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex

Ulven, J. B., and Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039

Verizon. (2022). 2022 data breach investigations report (DBIR). https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

Wash, R., Rader, E., Mandia, K., & Fossen, T. (2017). Prioritizing security over usability: Strategies for how people choose passwords. Journal of Cybersecurity, 3(1), 1–13. https://doi.org/10.1093/cybsec/tyab012

Mathews, A., & Haque, S. M. T. (2024). Exploring the risks of password reuse across websites of different importance. In Proceedings of the AHFE International Conference on Human Factors in Cybersecurity (pp. 5469–5478). AHFE International. https://doi.org/10.54941/ahfe1005469

Marcatto, F., Mistichelli, F., & Ferrante, D. (2025). Perceiving digital threats and artificial intelligence: A psychometric approach to cyber risk. Cybersecurity and Privacy, 5(4), 93. https://doi.org/10.3390/jcp5040093