Characterizing Cybersecurity Awareness Among Brazilian Computer Science Higher Education Students

Vinícius E. Ferreira[1], Edson OliveiraJr[1], Bruno B. Zarpelão[2], Avelino F. Zorzo[3]

[1]Informatics Department, State University of Maringá (UEM) – Maringá-PR – Brazil

[2]Computer Science Department, State University of Londrina (UEL) – Londrina-PR – Brazil

[3]Computing Department, PUCRS – Porto Alegre – RS – Brazil

vinicius.vef@gmail.com, edson@din.uem.br
brunozarpelao@uel.br, avelino.zorzo@pucrs.br

Abstract. *This study examines the cybersecurity awareness of Brazilian students at various academic levels, focusing on their understanding of fundamental concepts such as common threats, security controls, and risk-related scenarios. We conducted a survey with 199 participants, including 155 undergraduates and 44 graduates, and evaluated their performance based on three levels of exposure to cybersecurity education: no prior exposure (n=36), one source of exposure (n=81), and two or more sources (n=82). The results reveal a significant correlation between exposure to cybersecurity education and improved performance. The mean percentage of correct answers increased from 72.11% for those with no exposure to 79.35% for those with one source and reached 85.07% for those with two or more sources. Furthermore, students consistently underestimated their knowledge on the topic, although this perception gap diminished with increased exposure. These findings highlight the need for incorporating comprehensive cybersecurity into Information Technology (IT) curricula to enhance awareness and reduce risks associated with professional negligence, particularly among future IT practitioners in Brazil.*

1. Introduction

Cybersecurity is not solely a technological problem; it is, in fact, a sociotechnological challenge [Triplett 2022]. Psychological, behavioral, and social aspects all play a critical role in the intricate human-machine relationship. In certain cultures, sharing personal data or accounts may be considered the norm, leading to heightened risks [Sangwan 2024]. These factors affect individuals in varying ways, and not only are the uneducated prone to errors, but overconfident specialists are also vulnerable. Unaware staff can threaten an organization even without the intention to cause harm; these employees are called unintentional insider threats (UIT).

The CERT Insider Threat Team defines an UIT as "a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems" [CERT Insider Threat Team 2013]. Beyond the business context, even a friend or relative can unknowingly act as a UIT, leading to incidents that could have been prevented with effective cybersecurity awareness training.

A compelling example of the importance of raising cybersecurity awareness was the *stuxnet* threat case. *Stuxnet*, was an incredibly complex worm often referred to as "the first cyber weapon" that was successfully delivered to the offline uranium enrichment facilities in Natanz, Iran. It managed to infect the programmable logic controllers (PLCs) responsible for controlling the uranium-enriching centrifuges through a USB flash drive that an employee unknowingly inserted into their computers [Zetter 2014], causing significant damage to Iran's nuclear program.

Investing in users' awareness about cybersecurity may be an effective mitigation for many cybersecurity risks. In this context, the term "cyber awareness" is used to refer to "the ability of the user to recognize and avoid behaviors that could compromise cybersecurity and to act wisely and cautiously to increase cybersecurity" [National Institute of Standards and Technology (NIST) 2023].

To investigate whether Brazilian students are properly aware of cybersecurity concepts, risks, and threats, we conducted a survey involving 199 students, divided into three groups based on their prior exposure to cybersecurity education: no exposure (n=36), one source of exposure (e.g., a course or training, n=81), and two or more sources (n=82).

Our study evaluates four research questions (RQs): awareness of common cybersecurity threats (RQ1), ability to identify risks in IT scenarios (RQ2), knowledge of security controls (RQ3), and self-perception of cybersecurity knowledge (RQ4). By analyzing the respondents' performance across these dimensions, we seek to identify strengths, gaps, and the impact of educational exposure on students' readiness. The findings aim to ensure that future IT professionals are equipped to recognize and address cybersecurity challenges effectively, thereby reducing the risks associated with human factors in professional or non-professional settings.

2. Related Work

Formal cybersecurity education is a global challenge. Studies in Poland [Szumski 2018] and the Netherlands [Witsenboer et al. 2022] demonstrate that a lack of institutional proactivity leads to the marginalization of formal knowledge, resulting in informal learning through the internet, friends, or family, which can foster harmful digital habits and perpetuate myths and fallacies about cybersecurity.

In the Brazilian context, this need for formal education is urgent. [Carvalho et al. 2017], in their research with the school community, indicated that although 95.2% of teachers consider training in Internet security important and 90.5% support its inclusion in the curriculum, either in basic computer science courses or as a dedicated subject, 55.6% had never addressed the topic, with 76% of these claiming unpreparedness. This gap in educational preparedness can have practical consequences, as evidenced by [Randel et al. 2024], who demonstrated that 62.81% of passwords belonging to faculty and administrative staff at a Brazilian university were vulnerable and did not meet basic security requirements, signaling the urgent need for awareness even among more highly educated strata.

Investigating further, an exploratory study by [Henklain et al. 2024] with students in northern Brazil revealed a general cybersecurity knowledge with an average of 66.42% correct answers, being slightly higher for computer science students (69.44%) and for those with previous courses in cybersecurity (70.04% vs. 65.50% for those who had not).

Concurrently, [Zwilling et al. 2022] internationally confirmed the positive correlation between knowledge, awareness, and protective behaviors, and the positive impact of cybersecurity programs on student awareness, a point that the present study also explores by investigating the influence of educational exposure levels on technology students. Additionally, the study by [Henklain et al. 2024] observed considerable insecurity among participants regarding their own answers and problematic password creation practices, such as repetition (7.76%) and limited use of varied characters, findings that resonate with the vulnerabilities pointed out by [Randel et al. 2024]. Given this scenario, which indicates both the perceived need for cybersecurity education and the existing fragility in knowledge and practices in Brazil, the present research seeks to deepen the understanding of the cybersecurity awareness level of IT students, the impact of educational exposure on their knowledge, which topics present the greatest challenges, and the self-perception of knowledge of these future technology professionals.

3. Research Methodology

The adopted methodology consists of an empirical study carried out as a survey, which follows the guidelines provided by [Ghazi et al. 2019, Shull et al. 2008].

3.1. Aim and Research Questions

Our research aims to assess students' awareness of cybersecurity threats and risks in Brazil. More specifically, we aimed to determine whether students at different academic levels (undergraduate and graduate) could correctly answer basic to moderately difficult questions on fundamental cybersecurity concepts, such as common threats, security controls, and risk-related scenarios. We focused on topics that are not exclusively discussed by cybersecurity professionals or enthusiasts but should be known by every IT professional.

The survey was built around four research questions, which are described next. **RQ1: Are students aware of common cybersecurity threats that target human factors?** enumerates threats that often exploit human factors, such as phishing, spam, and ransomware, and assesses whether the respondents know their definitions. **RQ2: Can students identify cybersecurity risks in basic IT scenarios?** explores another dimension of cyber awareness among IT students by assessing whether respondents can recognize basic risks when using computational tools and resources. To evaluate this, the survey presented scenarios, such as a browser screen displaying a typosquatting attack attempt, to determine whether respondents could identify the risk. **RQ3: Are students aware of common information security controls?** examines the respondents' knowledge of core cybersecurity concepts and security controls, including firewalls, backups, hashing, and cryptography. Finally, **RQ4: Do students have a correct perception of their cybersecurity knowledge?** seeks to analyze whether the respondents' expectations about their level of knowledge in cybersecurity are aligned with their performance when answering the provided questions.

3.2. Survey Implementation

The survey was conducted through an online questionnaire with 45 questions divided into four sections. Sections 1 and 2 collected the respondents' consent to the questionnaire terms, along with demographic, professional, and academic information.

Section 3 covered RQ1, RQ2, and RQ3. All questions were multiple-choice and followed one of two formats. In the first format, the question tested the respondents' knowledge of a definition or basic concept, such as "What is spam?" or "What is a firewall?". For these questions, the answer choices included three incorrect options and one correct, along with a fifth option: "I have no idea". These responses allowed us to assess whether the respondent was confident in their answer (i.e., they did not select "I have no idea") and whether they knew the correct answer. The second format presented scenarios where respondents had to determine whether a cybersecurity risk was present. For example, one question displayed a browser screen with the *amazon.com.br* layout and asked whether the website looked legitimate. In this case, the URL contained a misspelling ("arnazon.com.br" instead of "amazon.com.br"), which indicates a fraudulent site. For these questions, respondents could only select "Yes" or "No".

Section 4 contained open-ended questions about the respondents' interest in cybersecurity and their self-perception of cybersecurity awareness related to RQ4.

Two cybersecurity experts reviewed the questionnaire before its online release. It was also pre-tested with a small group of students to ensure the questions were understood as intended. The questionnaire was emailed to higher education institutions (through coordinators of undergraduate and graduate technology courses) and mailing lists of organizations such as the Brazilian Computer Society. Additionally, it was posted on LinkedIn and WhatsApp groups for technology students. The survey was implemented using Google Forms.

4. Results

This section presents the results of our survey.

4.1. Demographics

The survey collected 203 responses, of which four were excluded due to being from non-IT respondents. This resulted in a total of 199 valid responses, comprising 155 undergraduate students (77.89%), spanning from first-year to final-year levels. The average number of students per academic year was 31, with a median of 30 and a standard deviation (SD) of 6.44. Additionally, 44 respondents (22.11%) were graduate students.

Participants came from twelve Brazilian states: Paraná (43.7%), Pernambuco (19.1%), Rio Grande do Sul (15.1%), Rio de Janeiro (10.6%), Amazonas (3.5%), Mato Grosso (3%), São Paulo (2%), Ceará (1%), Sergipe (0.5%), Pará (0.5%), Santa Catarina (0.5%), and Federal District (0.5%).

The mean age was 25.3 years (SD = 7.86), ranging from 17 to 57 with a median of 22. Regarding gender, 158 (79.39%) were male, 37 (18.59%) female, and 4 (2,01%) preferred not to inform. Among the respondents, 108 (54.27%) were employed: 54 (50%) in-person, 28 (25.92%) hybrid, and 26 (24.07%) remote, referring to their work setup. Regarding employer-provided cybersecurity training, 142 (71.35%) received none, while 57 (28.65%) did. Additionally, 125 (62.81%) sought cybersecurity education independently, and 74 (37.19%) did not.

4.2. Overall Results

The full sample analysis showed that the mean percentage of correct responses was 80.4%. Per research question 3.1, RQ1 outcome was 75.97%, RQ2 80.21%, RQ3 83.08%,

and RQ4 -16.17 p.p. In RQ4, the **negative** values indicate underestimation (knowledge exceeds self-estimate), **positive** values indicate overestimation (self-estimate exceeds knowledge). The -16.17 p.p. suggests participants underestimated their knowledge, outperforming their predictions, possibly due to the topic's complexity, reflecting the gap between actual and self-assessed knowledge.

Among undergraduates, student seniority was inversely proportional, with more freshmen than seniors. Segmenting undergraduates by seniority reveals a progressive improvement in accuracy means, as shown in Figure 1, likely tied to their maturity, exposure to computer science, and/or cybersecurity knowledge.

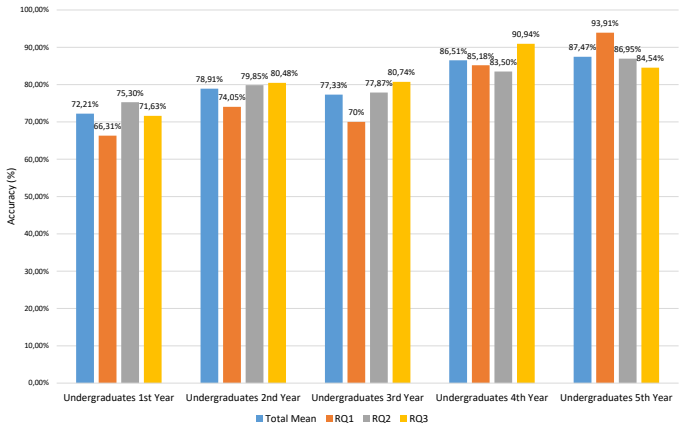

Figure 1. Undergraduate students - performance by academic year (in percentage)

Analyzing only graduate students, the evaluation showed an overall accuracy of 83.36%, with 80.9% for RQ1, 79.75% for RQ2, 89.14% for RQ3, and -15.69 p.p. for RQ4. The results for undergraduates (80%) and graduates (83.36%) show a similar overall performance. However, larger gaps in RQ1 (6.32 p.p.) and RQ3 (7.78 p.p.) suggest graduates' greater exposure to concepts. In comparison, RQ2's proximity (0.60 p.p.) indicates that the time and/or exposure were not sufficient to demonstrate an improvement in the accuracy rate of detecting risk situations in practical scenarios, representing a plateau that may indicate the need for educational content aligned with this gap.

4.3. Results by relevant exposure

This study measured participants' cybersecurity knowledge exposure using three variables: (1) participation in mandatory or elective cybersecurity courses, (2) proactive engagement in free courses or educational materials, and (3) cybersecurity training received in current or past jobs.

Data were organized for analysis per research question (RQ) using binary notation for each variable—Discipline, Free Course, Training—where "1" indicates exposure and "0" indicates none (e.g., 000: no exposure; 100: discipline exposure; 111: all three). Due to small sample sizes in some groups (e.g., "001" with six members), participants were aggregated into three categories: Group 0 ("No exposure"), Group 1 ("One source"), and Group 2 ("Two or more sources"), as shown in Table 1. Table 2 was added to detail outlier responses, enhancing the discussion.

Table 1. Weighted segmentation of groups by cybersecurity knowledge exposure

Group 0 - No exposure (000)					
Total	**Overall means (%)**	**RQ1 (%)**	**RQ2 (%)**	**RQ3 (%)**	**RQ4 (p.p.)**
36	72.11	66.66	74.24	72.53	-21
Group 1 - One source of exposure (001, 010, 100)					
Total	**Overall mean (%)**	**RQ1 (%)**	**RQ2 (%)**	**RQ3 (%)**	**RQ4 (p.p.)**
81	79.35	73.82	78.22	83.81	-17.73
Group 2 - Two or more sources of exposure (011, 101, 110, 111)					
Total	**Overall mean (%)**	**RQ1 (%)**	**RQ2 (%)**	**RQ3 (%)**	**RQ4 (p.p.)**
82	85.07	82.19	84.81	87	-12.39

Table 2. Detailed questions for discussion

Group 0 - No exposure (000)				
RQ	**Question**	**Score (%)**	**Never heard of (%)**	**Errors (%)**
RQ1	1	61.11	25.00	13.89
RQ1	14	75.00	25.00	0.00
RQ1	25	25.00	69.44	5.55
RQ2	3	72.22	-	27.77
RQ2	10	63.89	-	36.11
RQ2	11	58.33	-	41.66
RQ2	13	41.67	-	58.33
RQ2	21	55.56	-	44.44
RQ3	15	13.89	44.44	41.66
RQ3	22	47.22	41.67	11.11
RQ3	23	55.56	33.33	11.11
Group 1 - One source of exposure (001, 010, 100)				
RQ	**Question**	**Score (%)**	**Never heard of (%)**	**Errors (%)**
RQ1	1	64.20	8.64	27.16
RQ1	14	88.89	11.11	0.00
RQ1	25	33.33	45.68	20.99
RQ2	3	75.30	-	24.69
RQ2	10	61.73	-	38.27
RQ2	11	59.26	-	40.74
RQ2	13	70.37	-	29.63
RQ2	21	72.84	-	27.16
RQ3	15	30.86	25.93	43.21
RQ3	22	67.90	22.22	9.88
RQ3	23	83.95	9.88	6.17
Group 2 - Two or more sources of exposure (011, 101, 110, 111)				
RQ	**Question**	**Score (%)**	**Never heard of (%)**	**Errors (%)**
RQ1	1	87.80	3.66	8.54
RQ1	14	92.68	6.10	1.22
RQ1	25	41.46	41.46	17.07
RQ2	3	80.48	-	19.51
RQ2	10	71.95	-	28.05
RQ2	11	71.95	-	28.05
RQ2	13	80.49	-	19.51
RQ2	21	85.37	-	14.63
RQ3	15	47.56	8.54	43.90
RQ3	22	79.27	15.85	4.88
RQ3	23	87.80	7.32	4.88

Table 1 shows that all groups had **negative RQ4 values**, consistent with the overall RQ4 result in Section 4.2. Across groups, those with two or more exposure sources had self-assessments closer to reality (-12.39 p.p.) yet still underestimated their skills.

A significant increase in **all means** correlates with higher exposure levels, suggesting that diverse learning sources, such as courses, free training, or workplace programs, enhance overall cybersecurity understanding. The **12.96 p.p.** gap in general means between Group 0 and Group 2 highlights the positive impact of multiple educational approaches. Performance improved across all RQs: 15.53 p.p. in RQ1, 10.57 p.p. in RQ2, 14.47 p.p. in RQ3, and self-perception rose from -21 p.p. to -12.39 p.p.

To better explore the results for each research question, Table 2 presents some questions with noteworthy results; however, it is important to highlight that there are other questions with beneficial results that, for the sake of objectivity, have not been included in this table.

4.3.1. Results of RQ1

As pointed out in Section 4.2, the overall RQ1 result was 75.97%, indicating good comprehension, but Table 2 highlights three notable outliers. **Question 1: "What is Phishing?"**, phishing is the act of deceiving someone into disclosing information, and it is a very common term, present in emails (such as 'Report Phishing' buttons) and in non-specialized media. Despite its commonality in tech, Group 0 scored only 61.11%, and Group 1 scored 64.20%. This is an alert as phishing is the top initial access technique for the second consecutive year [ReliaQuest 2025]."Group 1, despite being exposed to a factor, did not show a much higher score than Group 0. The rate of 'Never heard of it' decreased from 25% to 8.64%, but the error rate increased from 13.89% to 27.16%, raising concerns about the correct understanding of the term. Accuracy rises significantly with exposure (26.69 p.p. from Group 0 to Group 2), and "Never heard of it" drops

sharply (25.00% to 3.66%), showing reduced uncertainty.

Question 14: "What is Ransomware?" Ransomware is malicious software that encrypts data and demands a ransom fee for the user to regain access, being one of the top threats extensively featured in both specialized and general media, with large-scale incidents prominently highlighted in numerous headlines over recent years. Performance is consistently high, with accuracy rising from 75.00% (Group 0) to 92.68% (Group 2), a 17.68 p.p. gain. The "Never heard of it" rate drops from 25.00% (Group 0) to 11.11% (Group 1) and then to 6.10% (Group 2), with errors at 0% in groups 0 and 1, and 1.22% in Group 2, suggesting ransomware is relatively well understood, even without exposure, but improves with more learning sources.

Question 25: "What is Zero Day?" Zero Day is a vulnerability exploited before the vendor's knowledge of its existence, leaving 'zero days' to patch it before threat actors start using it, being present in patch/update notes, and one of the most important reasons why you should update your software as soon as possible. This question reveals a significant gap. Accuracy remains low, rising from 25.00% (Group 0) to 41.46% (Group 2), a 16.46 p.p. increase. The high "Never heard of it" rate (69.44% in Group 0, still 41.46% in Group 2) indicates that "Zero Day", despite its prominence in vulnerability bulletins and news, remains poorly addressed in learning sources.

4.3.2. Results of RQ2

RQ2's overall performance was 80.21%, a 4.24 p.p. improvement over RQ1. Table 2 highlights four questions.

Question 3: "What is the safest password?" Passwords are a routine aspect of the numerous services that currently require authentication. Weak or reused passwords pose a significant risk to organizations; for instance, a compromised corporate email through a weak password can be used for social engineering attacks, password recovery for other accounts, and the exfiltration of sensitive data. The errors decreased from 27.77% to 24.69% and 19.51% in Groups 0, 1, and 2, respectively. This data reveals that even among those who had exposure to two or more sources of cybersecurity education, the errors are still high. Understanding password complexity is essential to avoid setting up weak passwords. In 2024, 85% of incidents involved compromised service accounts [ReliaQuest 2025], highlighting the importance of strong authentication methods to avoid invasions.

Question 10: "Does this website represent any data risks? (image of a browser with the Amazon website with typo)" scores rise from 63.89% to 71.95% (8.06 p.p.), but errors stay consistently high (36.11%, 38.27%, and 28.05% in Groups 0, 1, and 2, respectively). These results show a very dangerous situation, falling for a cloned website can lead to data leaks, business e-mail compromise, credit card fraud, and many others.

Question 11: "Browser with Magazine Luiza site image with typo" mirrors Question 10, with a 13.62 p.p. rise from Group 0 to Group 2, yet errors remain high (41.66%, 40.74%, and 28.05% in Groups 0, 1, and 2, respectively). Consistency between Q10 and Q11 suggests widespread difficulty in identifying *typosquatting* and similar URLs.

Question 13: "Email Extension Recognition": The largest improvement occurs here, accuracy rises from 41.67% to 70.37% and to 80.49% in Groups 0, 1 and 2, respectively. This is a 38.82 p.p. improvement from Group 0 to Group 2, with a notable jump between Group 0 and Group 1 (28.70 p.p.). However, a 19.51% error rate in Group 2 indicates persistent difficulty in recognizing potentially dangerous extensions. This metric may indicate a false sense of security when dealing with emails from unknown senders. Opening attachments with potentially malicious file extensions can quickly compromise the security of a computational environment.

Question 21: "Piracy Risks": Performance improves steadily (29.81 p.p. from Group 0 to Group 2), with errors dropping from 44.44% to 27.16% to 14.63% in Groups 0, 1, and 2, respectively, indicating that exposure raises piracy risk awareness. However, 14.63% is still a high error rate. Using pirated software can compromise security, as 'cracks' may contain unknown access points or threats.

4.3.3. Results of RQ3

RQ3 scored the highest overall performance at 83.08%. Table 2 highlights three questions.

Question 15: "Security Triad": The Confidentiality-Integrity-Availability (C-I-A) model is one of the foundational concepts in information security, allowing one to classify and understand the impacts of a threat. Performance is low across groups, accuracy rises from 13.89% to 47.56% (33.67 p.p.) from Group 0 to Group 2, but errors remain high (41.66%, 43.21% and 43.90% in Groups 0, 1 and 2 respectively). As shown in Table 2, Group 0 had 44.44% "Never heard of it" following a decrease to 25.93% in Group 1 and 8.54% in Group 2, showing persistent theoretical difficulty.

Question 22: "What is Hash"?: A hash is a fixed-length output generated by a mathematical function, designed to uniquely represent input data of any size and ensure data integrity through one-way transformations, present in many subjects in Computer Science, such as databases and cryptography. There is a notable improvement (32.05 p.p. from Group 0 to Group 2), with "Never heard of it" falling from 41.67% to 15.85%. As this concept is present in other disciplines and is not limited to information security, an improvement in the score was expected. However, 15.85% 'Never heard of it' is a relevant statistic for those who had two or more variables of exposure to cybersecurity education, considering that hashing is an important tool for ensuring the integrity of transferred files and securely storing passwords, among other applications.

Question 23: "What is Log"?: Log is a chronological record of events, actions, or messages generated by software or systems, used to monitor performance or troubleshoot issues, a foundational concept in Computer Science. There was a significant gain (32.24 p.p.) from Group 0 to Group 2, with "Never heard of it" reduced from 33.33% to 7.32%. Similar to question 22, this concept is explored among multiples subjects in Computer Science, however 83.95% and 87.8% of accuracy among Group 1 and Group 2 respectively indicates a gap in knowledge, as logs are of extreme importance within cybersecurity.

4.3.4. Results of RQ4

All groups underestimated their performance. Table 1 suggests that exposure improves recognition of abilities, with self-perception rising 8.61 p.p. from Group 0 to Group 2. This result aligns with the findings on self-evaluation reported by [Henklain et al. 2024].

5. Discussion of Results

In line with our expectations, exposure to cybersecurity concepts has been associated with improved performance compared to individuals with no exposure. However, significant knowledge gaps persist even among those exposed to multiple sources of information. For instance, in Group 2 (individuals with two or more sources of exposure), **40% of the questions exhibit error rates exceeding 14%**, highlighting the need for a stronger grasp of fundamental concepts that serve as the basis for more advanced knowledge.

There are significant challenges within the RQ2 questions. 19.5% of respondents failed to identify the most secure password, this data corroborates with [Randel et al. 2024] and [Henklain et al. 2024] findings; 28% were unable to recognize a fraudulent webpage; 19.5% struggled to identify file extensions that could be malicious; and 14.6% could not grasp the risks associated with piracy practices. In addition, 26.8% of members of Group 2 failed to identify the risks linked to the Bring Your Own Device (BYOD) policy, 14% mistakenly identified the function of a firewall, another 14% were unable to verify the authenticity of a secure webpage, and 9% did not recognize HTTPS as a secure browsing protocol.

As technology grows increasingly complex, these situations can expose computational environments to substantial financial and reputational risks. Simultaneously, cybersecurity awareness is particularly critical for higher education students. Employer-provided cybersecurity training is notably scarce. Only 28.65% of students reported receiving any training, probably due to budget constraints or a general lack of awareness of its importance.

To bridge these gaps, educational institutions should consider developing comprehensive cybersecurity awareness campaigns. Strategies such as lectures, simulations, interdisciplinary events, hackathons, and Capture the Flag (CTF) competitions have proven effective in fostering discussion and enhancing participants' awareness. Although these initiatives provide valuable learning experiences [Chothia and Novakovic 2015], they demand significant resources and must be carefully tailored to the specific context and needs of each institution [Ernits and Kikkas 2016].

6. Threats to Validity

One common threat in survey-based research is the possibility of respondents misunderstanding the questions. To minimize this issue, we conducted a pilot study with a small group of students before releasing the questionnaire online. Additionally, we provided contextual explanations for most questions and ensured that the terminology used was appropriate for the target audience. Despite these efforts, we acknowledge that some respondents may have faced difficulties in interpreting some questions. Another limitation concerns the possibility that respondents used external resources while completing the questionnaire. Since the survey was implemented online without direct supervision, participants could have searched for answers online or used AI-based

tools such as ChatGPT. This could affect the accuracy of self-reported knowledge and awareness.

The possibility of having respondents outside the target population (Brazilian students) also threatened validity. To address this issue, we included questions about the academic and professional profiles of respondents, which would allow us to filter out individuals who did not meet the study's criteria. However, we cannot entirely rule out the possibility that some respondents provided inaccurate information about their academic status.

Sampling bias represents another important limitation. To mitigate this issue, we disseminated the questionnaire through various channels with national reach. This strategy was somewhat effective, as we received responses from all Brazilian regions. Nonetheless, many respondents were from Paraná, which does not reflect the geographical distribution of technology students across Brazil. This imbalance is likely due to the authors' affiliations with universities in Southern Brazil, which facilitates access to local academic networks. Furthermore, the sample size of 203 respondents can be considered substantial given the challenges of obtaining online voluntary responses for a 45-question survey. However, it may still be insufficient to fully represent the broader population of technology students in Brazil.

Despite these limitations, the measures taken to enhance the reliability of our survey contribute to the validity of our findings. As the first survey with this objective, this study represents an important contribution.

7. Final Remarks

This study presented an evaluation of the basic cybersecurity knowledge among higher education students. As expected, the results demonstrated improvements corresponding to the level of exposure to cybersecurity education; however, even among the more educated, certain questions still exhibited high error or unfamiliarity rates, indicating a gap in practical knowledge on both technical and behavioral issues. These statistics are relevant for guiding the development of educational material in the field of cybersecurity to address current students' challenges while also presenting opportunities for further research to gain a deeper understanding of the teaching and learning dynamics in this constantly evolving domain.

Data Availability

Data from this survey is available at https://doi.org/10.5281/zenodo.15498787.

Acknowledgments

The authors deeply thank the **educators and professionals** for their valuable time spent participating in this research. This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. Edson OliveiraJr thanks CNPq/Brazil support (Grant #311503/2022-5). Avelino F. Zorzo thanks CNPq/Brazil support (Grant #306250/2021-7).

References

Carvalho, E., Reis, T., and Alves, F. (2017). Ensino de noções básicas de segurança da informação nas escolas brasileiras. In *Anais do XXIII Workshop de Informática na Escola*, pages 765–774, Porto Alegre, RS, Brasil. SBC.

CERT Insider Threat Team (2013). Unintentional insider threats: A foundational study. Technical Note CMU/SEI-2013-TN-022, Carnegie Mellon University, Pittsburgh. Available online.

Chothia, T. and Novakovic, C. (2015). An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. In *3GSE15 Summit Program, USENIX Conference*. Accessed: March 24, 2025.

Ernits, M. and Kikkas, K. (2016). A live virtual simulator for teaching cybersecurity to information technology students. In Zaphiris, P. and Ioannou, A., editors, *Learning and Collaboration Technologies*, pages 474–486, Cham. Springer International Publishing.

Ghazi, A. N., Petersen, K., Reddy, S. S. V. R., and Nekkanti, H. (2019). Survey research in software engineering: Problems and mitigation strategies. *IEEE Access*, 7:24703–24718.

Henklain, M., Lobo, F., Feitosa, E., Cavalcante, L., Alencar, J., Bríglia, V., Araújo, G., and Alves, G. (2024). Caracterização de conhecimentos e comportamentos de cibersegurança: Estudo exploratório com dados predominantes do extremo norte brasileiro. In *Anais do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 76–91, Porto Alegre, RS, Brasil. SBC.

National Institute of Standards and Technology (NIST) (2023). Special publication 800-50 revision 1: Building an information technology security awareness and training program. Technical report, NIST. Accessed: March 24, 2025.

Randel, J., Serrão, J., Romão, H., Lobo, F., Henklain, M., and Feitosa, E. (2024). Caracterização de senhas utilizadas pela comunidade universitária como ponto de partida para o desenvolvimento de capacitação em cibersegurança. In *Anais do XXXII Workshop sobre Educação em Computação*, pages 680–691, Porto Alegre, RS, Brasil. SBC.

ReliaQuest (2025). Reliaquest annual cyber-threat report 2025. Technical report, ReliaQuest. Accessed: March 24, 2025.

Sangwan, A. (2024). Human factors in cybersecurity awareness. In *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, pages 1–7.

Shull, F., Singer, J., and Sjøberg, D. I. (2008). *Guide to advanced empirical software engineering*, volume 93. Springer.

Szumski, O. (2018). Cybersecurity best practices among polish students. *Procedia Computer Science*, 126:1271–1280. Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 22nd International Conference, KES-2018, Belgrade, Serbia.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2(3):573–586.

Witsenboer, J. W. A., Sijtsma, K., and Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the netherlands. *Computers & Education*, 186:104536.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishers, a division of Random House LLC, New York.

Zwilling, M., Klien, G., Lesjak, D., Łukasz Wiechetek, Cetin, F., and and, H. N. B. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1):82–97.