E-ISSN 2520-0429
ISSN 2519-1284

European Journal of Economics, Law and Social Sciences

Vol.10 No.1
January, 2026

Research Article

Empowering Digital Defense: The Role of Cyber-Vaccination and Awareness Training in Strengthening Cybersecurity in the Modern Era
Awareness Training for Cybersecurity

Anni Dasho Sharko
Luarasi University (Albania)

Folitjona Puravelli
Luarasi University (Albania)

Genci Sharko
Polytechnic University of Tirana (Albania)

DOI: https://doi.org/10.2478/ejels-2026-0003

Abstract

Today's rapidly evolving digital world has experienced a steady increase in the threat of hacking. As cyberattacks become more frequent and sophisticated, cyber-vaccination technology is being developed as a security method to counter the potential dangers posed by botnets. Cyber-vaccination involves exposing individuals to simulated cyberattacks, allowing them to become familiar with common threats and learn how to respond appropriately. Through internet safety awareness training, participants develop essential skills that are critical for maintaining online security.

On a global scale, the growth of cybercrime mirrors the rapid spread of an infectious virus. Based on reported financial losses, cybercriminals appear to be accumulating increasing amounts of stolen funds each year. Although a wide range of advanced technologies exists to identify and prevent known cyber threats, these measures are often insufficient when attackers exploit human behavior as their primary method of intrusion.

Many reputable organizations invest significant resources in training their employees to recognize and avoid phishing emails and other forms of cyberattacks. These organizations allocate funding and establish specialized teams to provide effective cybersecurity education. However, a substantial portion of the general population lacks access to such routine training, which presents a significant challenge.

Providing accessible cybersecurity education is therefore essential. This study aims to examine the various free training options currently available, as well as the common risks and challenges associated with these educational opportunities. Additionally, the study will compare alternative solutions to determine their effectiveness in improving cybersecurity awareness.

Keywords: Cybersecurity questionnaire, information communication, cybersecurity awareness, higher education.

1. Introduction

Advancements in contemporary information-sharing technologies have significantly enhanced both the quality and reach of information dissemination. As a result, acquiring knowledge has become more efficient and accessible. However, the widespread distribution of information through modern communication channels and advanced technological tools has also contributed to the emergence of new cybersecurity challenges. Consequently, data breaches and the misuse of stolen information have become increasingly serious concerns in the era of information modernization. Safeguarding data privacy within computer networks is therefore critical, particularly in institutions with large user populations, such as universities, where students are the primary users of information systems. Cybersecurity breaches in higher education can result in personal data violations and various forms of digital exploitation, including the theft and misuse of intellectual property.

The rapid advancement of modern technology has fundamentally transformed work practices and perceptions of communication and information exchange. Numerous communication systems have been developed and implemented to support administrative and academic functions within universities (Baranyi et al., 2021). As a result, both public and private higher education institutions—especially following the COVID-19 pandemic—have introduced a variety of digital services and adopted new technologies to ensure continuous access to educational resources regardless of time or location (Bauman et al., 2018).

In parallel, there has been a substantial increase in cybercrime activities carried out by organized groups employing increasingly sophisticated methods to exploit digital systems (Chen et al., 2023). Financial gain remains the primary motivation for hacking, achieved through the acquisition of valuable data that is later monetized, often via illicit markets on the dark web. This trend has intensified the exploitation of stolen information, thereby endangering cyberspace and exposing organizations to significant legal and financial liabilities.

Cybersecurity must be regarded as a critical responsibility across all organizational departments, not solely within information technology units. Employees play a pivotal role in maintaining cybersecurity by adhering to institutional security policies and procedures. Failure to do so has contributed to the growing number of cybersecurity incidents. Human behavior remains the most vulnerable element within organizations, as staff actions can unintentionally expose institutional assets to both internal and external threats. Indeed, human error is among the primary means by which attackers gain access to otherwise secure systems (Amoresano & Yankson, 2023).

In recent years, Western Balkan countries have faced an escalation in cybersecurity threats targeting essential government services. Albania, in particular, has experienced

significant cyberattacks on its government information technology infrastructure, leading to a temporary partial disruption of the e-Albania digital services platform. Given the increasing prevalence of cyber threats and cybercrime, prioritizing cybersecurity awareness across the Western Balkans has become imperative. Additionally, examining cybersecurity awareness among university students is essential, as educational institutions have experienced a growing number of attempts to bypass information system security. Addressing these challenges requires increased institutional effort and financial investment to maintain and enhance security infrastructures, as well as a deeper understanding of the implications of cybercrime in higher education.

At Luarasi University, an assessment was conducted to evaluate student behavior regarding cybersecurity awareness and compliance with established security guidelines. A customized questionnaire was developed to examine various aspects of cybersecurity through a carefully designed survey. The purpose of this instrument was to assess students' knowledge of cybercrime and protection mechanisms, identify gaps in awareness, and determine the need for further education and training. The questionnaire employed quantitative research methods and statistical analysis to evaluate the collected data and draw meaningful conclusions. It addressed multiple security concerns, including protection against computer viruses, phishing attempts, deceptive advertisements, pop-up windows, and risks associated with electronic communications. The findings indicate an urgent need for comprehensive educational initiatives to improve student awareness of personal data privacy risks (Solic et al., 2024; Khando et al., 2021).

Implementing targeted cybersecurity training is essential for fostering student confidence in the secure and reliable use of university information systems. Accordingly, a thorough evaluation was conducted to educate students on best cybersecurity practices and highlight existing vulnerabilities in computer networks (Alharbi & Tassaddiq, 2021). Based on the survey analysis and findings, this study aims to strengthen academic initiatives that enhance students' understanding of cybersecurity and increase awareness of the risks and challenges associated with the secure use of digital technologies in higher education environments (Blum, 2020).

2. **Methodology**

a) Research Tools

An electronic questionnaire administered through an online survey was employed to ensure the efficient collection of high-quality data regarding cybersecurity usage and awareness among students at Luarasi University. This approach enabled rapid data collection from a large and geographically diverse student population.

The survey consisted of 40 questions covering a broad range of cybersecurity-related topics, organized into the following categories:

a. Cybersecurity knowledge (5 questions)
b. Use of security tools (5 questions)
c. Internet usage (5 questions)

d. Cryptology (5 questions)
e. Phishing awareness (5 questions)
f. Social media use (5 questions)
g. Browser security (5 questions)
h. Demographics (5 questions)

The initial pool of survey questions was preselected based on prior academic research in the field of cybersecurity (Alrobaian et al., 2023). Organizing the questionnaire into thematic sections allowed for the examination of multiple aspects of internet usage and cybersecurity practices. The grouping of questions related to security tools enabled an assessment of Luarasi University's compliance with established security protocols. Students' responses also provided insights into their understanding of computer viruses and phishing attacks.

Additionally, questions related to safe online browsing were designed to evaluate students' awareness of the security features provided by commonly used web browsers. A significant portion of the questionnaire assessed students' understanding of potential risks associated with social media platforms and their ability to respond appropriately to cybercrime incidents. Overall, the survey facilitated a comprehensive evaluation of students' knowledge, skills, behaviors, attitudes, and self-perceptions related to cybersecurity (Umeugo, 2023).

b) Research Environment and Participants

To ensure clarity and validity, the survey was initially developed in Albanian and subsequently translated into English (Kida & Karaj, 2020; Milin, 2022). Prior to the final quantitative and qualitative analysis, two rounds of pilot testing were conducted to evaluate the questionnaire's clarity, feasibility, and accuracy. Feedback obtained during this phase was carefully reviewed and used to refine and restructure the survey items, resulting in improved overall quality.

Based on pilot testing outcomes, the final questionnaire was adapted to accommodate students from diverse educational backgrounds. The response format was simplified to minimize completion time while maintaining accuracy and reliability.

To facilitate broader participation, a Memorandum of Understanding (MoU) was established to collaborate with 50 students from different universities, who were provided with electronic versions of the survey. At Luarasi University, the Faculty of Information Technology and Innovation includes three departments: Business Informatics, Information Technology and Innovations, and Mathematics and Statistics. An initial random selection of five students was conducted, followed by a final selection of students from three additional faculties—Law, Economics, and Medical Sciences—to ensure disciplinary diversity.

The finalized questionnaire included 40 focused questions, supplemented by definitions and explanations of cybersecurity-related terminology to assist comprehension. This design enabled students, including those without prior technical expertise, to complete the survey effectively. The questionnaire was developed and distributed using the Microsoft Teams Forms platform. From the outset, participants

were informed of the survey's objectives.
A working group comprising faculty deans and staff members was established to support the organization and distribution of the survey and to facilitate student participation. Through this coordinated effort, more than 1,000 students from Luarasi University completed the online questionnaire, resulting in a robust dataset that enhanced the reliability and accuracy of the findings.

c) Research Design and Respondent Perceptions
After evaluating several methodological approaches for assessing cybersecurity awareness through online surveys, a multi-layered survey design with structured question groupings was adopted to ensure clarity, accuracy, and reliability (Ikart, 2019). The pilot testing phase played a critical role in refining the questionnaire based on student feedback, ultimately improving the quality of the final instrument. Following these revisions, the finalized questionnaire was distributed electronically.
The survey results indicate that Luarasi University's initiatives to promote cybersecurity awareness and educate students on digital security practices have been effective. Respondents were also asked to evaluate their level of satisfaction and engagement with the survey using a five-point Likert scale (strongly agree, agree, neutral, disagree, strongly disagree).
As illustrated in Figure 1, the majority of respondents found the survey engaging and informative, with only a small percentage expressing a lack of interest. According to the final analysis, approximately 85% of participants reported a high level of enthusiasm and satisfaction with the survey's content and structure, indicating strong engagement and perceived value.

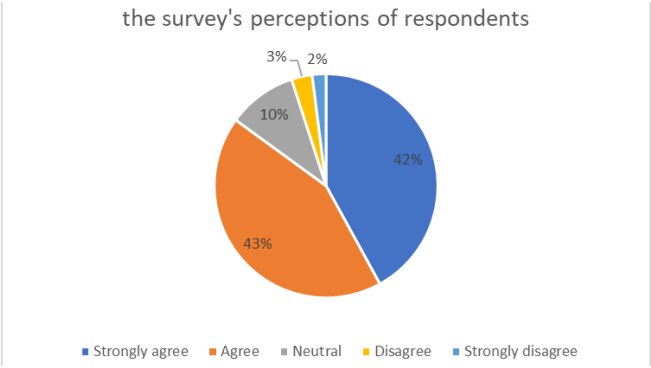

Fig 1. Survey's perceptions of respondents

3. The Outcomes

A representative sample of students was selected to reflect the overall student population of Luarasi University. Statistical distribution methods were applied to ensure inclusivity across key variables, including cybersecurity principles, countermeasures, password management, and internet navigation practices. All

students registered for the academic year were eligible to participate.
Demographic variables such as gender and age were considered in the analysis (Aslan et al., 2023). The demographic characteristics of the study participants are summarized in Table 1, which presents an overview of the respondents' profiles.

Table 1. Demographic information of research respondents.

Variables		**Number**	**Percentage %**
Sex	Male	550	55
(Male-Female)	Female	450	45
Age (years)	18–21	750	75
	22–30	250	25
Type of Faculty/ Department	Faculty of Information Technology and Innovation/Department of Business Informatics (Number of IT/AI/ Cybersecurity = 7)	250	25
	Faculty of Information Technology and Innovation/Department of Information Technology and Innovation/ (Number of IT/AI/Cybersecurity = 7)	250	25
	Faculty of Economics (Number of IT/AI/Cybersecurity = 0)	100	10
	Faculty of Law (Number of IT/AI/ Cybersecurity = 0)	100	10
	Faculty of Medical Sciences/Department of Dentistry (Number of IT/AI/Cybersecurity = 0)	100	10
	Faculty of Medical Sciences/Department of Nursing (Number of IT/ AI/Cybersecurity = 0)	100	10
	Faculty of Medical Sciences/Department of Pharmacy (Number of IT/AI/Cybersecurity = 0)	100	10

Variables		Number	Percentage %
Year of Study	1st year	300	30
	2nd year	300	30
	3rd year	200	20
	4th year	100	10
	5th year	100	10
Daily Used Device	Smartphone	700	70
	Tablet	100	10
	Desktop	100	10
	Laptop	100	10

The survey results indicate that the predominant age group of participants (75%) was between 18 and 21 years, which aligns with the average age of students at Luarasi University. The findings further revealed that male participation exceeded female participation, with a distribution of 55% and 45%, respectively. Additionally, the majority of participating students (70%) reported using smartphones as their primary device for daily activities, whereas laptops were used by a smaller proportion of students (10%) as the most frequently used secondary device.

3.1 *Understanding of Fundamental Cybersecurity Principles*

Cybersecurity is founded on three fundamental principles—confidentiality, integrity, and availability—commonly referred to as the CIA triad. All devices and services with direct internet connectivity must implement these three principles through the adoption of secure protocols and procedures. Given the increasingly sophisticated techniques employed by hackers in recent years, it is imperative for academic institutions, including universities, to adopt effective measures to protect their networks and sensitive data from cyberattacks (Cremer et al., 2022). This study aimed to evaluate students' understanding of fundamental cybersecurity principles, as students are the primary users of information technology assets within educational institutions.

Table 2 presents findings indicating that 44.4% of students manually update applications on their hardware devices, while 43.1% rely on automatic updates to maintain current software. However, a notable proportion of respondents (approximately 4.6%) reported that they do not update their applications or operating systems. This lack of updating poses significant security risks, potentially exposing both individual devices and the university's digital infrastructure to future cyber threats and data breaches.

Table 2: Outcome of the question "How do you update your device?"

Variable	Frequency	Percentage (%)
Update automatically (without user input)	431	43.1
Manual update (the user turns off automatic updates and only updates old software when they need to)	444	44.4
No update (the user doesn't install the updates that are needed)	46	4.6
Update that you forgot (User doesn't care about updates at all)	79	7.9

The survey results indicate that students spend a considerable amount of time using mobile phones and computers for information retrieval and online communication. Despite their regular academic commitments, students reported spending approximately four to eight hours per day using their smartphones and laptops. This duration often increases substantially during periods of free time.

4. Conclusion

The findings suggest that a significant proportion of users in Albania lack familiarity with fundamental cybersecurity concepts and best practices for protecting their devices from malware, viruses, and fraudulent activities. This deficiency is concerning, given the increasing importance of cybersecurity in today's digital environment. Consequently, higher education institutions across the country must prioritize the protection of sensitive information as a critical institutional responsibility.

The primary objective of this study was to assess the level of cybersecurity competence among students enrolled at Luarasi University in Albania. To achieve this objective, a quantitative research methodology was employed. The results of the statistical analysis indicate that senior administrators and institutional managers should actively promote and implement comprehensive cybersecurity awareness and training programs for students. These initiatives should be integrated into the

university's broader security management framework.

Academic institutions are expected to provide ongoing security awareness education and training sessions to ensure that users understand the most significant cybersecurity vulnerabilities and risks. Such initiatives are essential for fostering a security-conscious culture within the academic environment.

In light of the study's findings, it is recommended that Luarasi University enhance students' understanding of common cybersecurity issues, including vulnerabilities, attacks, and security incidents, in order to strengthen their overall security posture. This recommendation represents a practical and feasible course of action based on the evidence gathered.

Passive awareness strategies—such as email notifications, oral presentations, newsletters, and text messages—are insufficient when used in isolation. While these methods contribute to information dissemination, they do not adequately ensure effective learning or behavioral change. Proactive approaches, including interactive workshops, interviews, and free online training programs, have been shown to be more effective than purely reactive measures. Therefore, it is strongly recommended that both passive and proactive strategies be implemented in combination to achieve the desired cybersecurity awareness and competency outcomes.

References

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), Article 23. https://doi.org/10.3390/bdcc5020023

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity awareness assessment among trainees of the Technical and Vocational Training Corporation. *Big Data and Cognitive Computing, 7*(2), Article 73. https://doi.org/10.3390/bdcc7020073

Amoresano, K., & Yankson, B. (2023). Human error: A critical contributing factor to the rise in data breaches—A case study of higher education. *HOLISTICA – Journal of Business and Public Administration, 14*(1), 1–15. https://doi.org/10.2478/hjbpa-2023-0007

Aslan, Ö., Aktuğ, S. S., Özkan-Okay, M., Yılmaz, A. A., & Akın, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), Article 1333. https://doi.org/10.3390/electronics12061333

Baranyi, P., Csapó, Á., Budai, T., & Wersényi, G. (2021). Introducing the concept of Internet of Digital Reality: Part I. *Acta Polytechnica Hungarica, 18*(7), 7–23. https://doi.org/10.12700/APH.18.7.2021.7.12

Bauman, A. A., & Shcherbina, N. V. (2018). Millennials, technology, and cross-cultural communication. *Journal of Higher Education Theory and Practice, 18*(3), 11–16. https://doi.org/10.33423/jhetp.v18i3.562

Blum, D. (2020). Strengthen security culture through communications and awareness programs. In *Rational cybersecurity for business* (pp. 59–74). Apress. https://doi.org/10.1007/978-1-4842-5952-8_4

Chen, S., Wang, J., Zhao, X., & Li, Y. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities & Social Communications, 10*(1), Article 225. https://doi.org/10.1057/s41599-023-01560-x

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., & Murphy, F. (2022). Cyber

risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance: Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Ikart, E. M. (2019). Survey questionnaire survey pretesting method: An evaluation of survey questionnaire via expert reviews technique. *Asian Journal of Social Science Studies, 4*(2), 1–8. https://doi.org/10.20849/ajsss.v4i2.565

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, Article 102267. https://doi.org/10.1016/j.cose.2021.102267

Kida, E. B., & Karaj, T. (2020). Development of an Albanian version of the questionnaire on teacher–student interaction. *Center for Educational Policy Studies Journal, 10*(3), 49–68. https://doi.org/10.26529/cepsj.451

Milin, V. (2022). Review of *Learning in educational context: Psychology of learning/teaching* by A. Ž. Pešikan. *Center for Educational Policy Studies Journal, 12*(3), 451–456. https://doi.org/10.26529/cepsj.1520

Solic, K., Velki, T., Fošić, I., & Vuković, M. (2024). Study on information security awareness using the Behavioral-Cognitive Internet Security Questionnaire. *Acta Polytechnica Hungarica, 21*(4), 47–65. https://doi.org/10.12700/APH.21.4.2024.4.3

Umeugo, W. (2023). Cybercrime awareness on social media: A comparative study. *International Journal of Network Security & Its Applications, 15*(2), 25–38. https://doi.org/10.5121/ijnsa.2023.15202