

Millenium, 2(27)

---




---

**REFORÇAR O ENSINO DA CIBERSEGURANÇA PARA ESTUDANTES UNIVERSITÁRIOS: COLMATAR AS VULNERABILIDADES E PROMOVER PRÁTICAS PROACTIVAS DE SEGURANÇA DIGITAL**

**STRENGTHENING CYBERSECURITY EDUCATION FOR UNIVERSITY STUDENTS: BRIDGING VULNERABILITIES AND PROMOTING PROACTIVE DIGITAL SAFETY PRACTICES**

**FORTALECIMIENTO DE LA EDUCACIÓN EN CIBERSEGURIDAD PARA ESTUDIANTES UNIVERSITARIOS: CERRANDO BRECHAS DE VULNERABILIDAD Y FOMENTANDO PRÁCTICAS**

Anxhela Ferhataj<sup>1</sup>  <https://orcid.org/0000-0002-1054-2351>

Fatmir Memaj<sup>2</sup>  <https://orcid.org/0000-0002-2156-0942>

Roland Sahatcija<sup>3</sup>  <https://orcid.org/0009-0005-8355-7676>

Ariel Ora<sup>3</sup>  <https://orcid.org/0009-0000-9669-8359>

<sup>1</sup> European University of Tirana, Tirana, Albania

<sup>2</sup> University of Tirana, Tirana, Albania

<sup>3</sup> Independent Researcher, Toronto, Canada

Anxhela Ferhataj - anxhela.ferhataj@uet.edu.al | Fatmir Memaj - fatmirmemaj@feut.edu.al | Roland Sahatcija - rrsahatcija@gmail.com |

Ariel Ora - arieloraa@gmail.com



---

**Corresponding Author:**

*Anxhela Ferhataj*

Khura Complex, St. Xhanfize Keko

1000 – Tirana - Albania

[anxhela.ferhataj@uet.edu.al](mailto:anxhela.ferhataj@uet.edu.al)

RECEIVED: 31<sup>st</sup> March, 2025

REVIEWED: 03<sup>rd</sup> June, 2025

ACCEPTED: 18<sup>th</sup> June, 2025

PUBLISHED: 25<sup>th</sup> July, 2025

DOI: <https://doi.org/10.29352/mill0227.41111>

## RESUMO

**Introdução:** À medida que os estudantes universitários em regiões emergentes como a Albânia se envolvem cada vez mais com plataformas digitais, enfrentam riscos crescentes de cibersegurança. Embora ferramentas básicas como o software antivírus sejam comuns, persistem lacunas críticas na gestão de senhas e na detecção de phishing, destacando a necessidade urgente de uma educação em cibersegurança aprimorada.

**Objetivo:** Examinar as lacunas nas práticas de cibersegurança entre os estudantes universitários e identificar áreas críticas que exigem maior atenção.

**Métodos:** Foi realizada uma pesquisa quantitativa com 242 estudantes de disciplinas relacionadas à TI. A pesquisa avaliou práticas de segurança digital, percepções de ameaças e respostas a incidentes de cibersegurança. Foi aplicado uma análise de regressão logística para avaliar a relação entre comportamentos proativos de cibersegurança e a redução de incidentes cibernéticos.

**Resultados:** Os resultados revelam uma lacuna notável na conscientização dos estudantes sobre os riscos de cibersegurança. Os estudantes são mais propensos a relatar incidentes de cibersegurança quando existem mecanismos de denúncia anônima, enfatizando o papel crucial dos sistemas que respeitam a privacidade para promover a denúncia proativa de incidentes dentro das universidades. Além disso, a análise de regressão logística mostra que os estudantes que se envolvem consistentemente em comportamentos proativos de cibersegurança têm significativamente menos probabilidade de encontrar ou relatar incidentes relacionados a malware, destacando ainda mais a importância de cultivar esses comportamentos para reduzir a exposição aos riscos cibernéticos.

**Conclusão:** A pesquisa enfatiza a necessidade de intervenções educacionais focadas em práticas avançadas de cibersegurança. Universidades devem integrar programas que fortaleçam a segurança digital, preparando os estudantes para os riscos digitais crescentes.

**Palavras-chave:** cibersegurança; segurança digital; percepções de ameaças; respostas comportamentais; ciberataques

## ABSTRACT

**Introduction:** As university students in emerging regions like Albania increasingly engage with digital platforms, they face growing cybersecurity risks. While basic tools like antivirus software are common, critical gaps in password management and phishing detection persist, underscoring the urgent need for enhanced cybersecurity education.

**Objective:** To examine the gaps in cybersecurity practices among university students and identify critical areas that need more focus.

**Methods:** A quantitative survey was conducted with 242 students from IT-related disciplines. The survey assessed digital security practices, threat perceptions, and responses to cybersecurity incidents. Logistic regression analysis was applied to evaluate the link between proactive cybersecurity behaviors and the reduction of cyber incidents.

**Results:** The findings reveal a notable gap in students' awareness of cybersecurity risks. Students are more inclined to report cybersecurity incidents when anonymous reporting mechanisms are available, emphasizing the crucial role of privacy-respecting systems in promoting proactive incident reporting within universities. Additionally, logistic regression analysis shows that students who consistently engage in proactive cybersecurity behaviors are significantly less likely to encounter or report malware-related incidents, further highlighting the importance of cultivating these behaviors to reduce exposure to cyber risks.

**Conclusion:** This study underscores the need for educational programs that focus on advanced cybersecurity practices. It advocates for universities to implement tailored curricula that enhance students' digital security competencies, better preparing them for evolving cyber risks.

**Keywords:** cybersecurity; digital safety; threat perceptions; behavioral responses; cyberattacks

## RESUMEN

**Introducción:** A medida que los estudiantes universitarios de regiones emergentes como Albania se involucran cada vez más con plataformas digitales, enfrentan riesgos crecientes de ciberseguridad. Si bien herramientas básicas como el software antivirus son comunes, persisten brechas críticas en la gestión de contraseñas y la detección de phishing, lo que resalta la urgente necesidad de una educación en ciberseguridad más robusta.

**Objetivo:** Examinar las brechas en las prácticas de ciberseguridad entre los estudiantes universitarios e identificar áreas críticas que requieren mayor atención.

**Métodos:** Se realizó una encuesta cuantitativa con 242 estudiantes de disciplinas relacionadas con las TI. La encuesta evaluó las prácticas de seguridad digital, la percepción de amenazas y las respuestas a incidentes de ciberseguridad. Se aplicó un análisis de regresión logística para evaluar la relación entre los comportamientos proactivos de ciberseguridad y la reducción de incidentes cibernéticos.

**Resultados:** Los hallazgos revelan una brecha notable en la conciencia de los estudiantes sobre los riesgos de ciberseguridad. Los estudiantes son más propensos a reportar incidentes de ciberseguridad cuando existen mecanismos de denuncia anónima, lo que subraya el papel crucial de los sistemas que respetan la privacidad para fomentar la denuncia proactiva de incidentes dentro de las universidades. Además, el análisis de regresión logística muestra que los estudiantes que participan consistentemente en comportamientos proactivos de ciberseguridad tienen significativamente menos probabilidades de encontrarse o reportar incidentes relacionados con malware, destacando aún más la importancia de cultivar estos comportamientos para reducir la exposición a riesgos cibernéticos.

**Conclusión:** La investigación enfatiza la necesidad de intervenciones educativas centradas en prácticas avanzadas de ciberseguridad. Las universidades deben integrar programas que fortalezcan la seguridad digital, preparando a los estudiantes para los crecientes riesgos digitales.

**Palabras Clave:** ciberseguridad; seguridad digital; percepciones de amenazas; respuestas comportamentales; ciberataques

DOI: <https://doi.org/10.29352/mill0227.41111>

## INTRODUCTION

Understanding the cybersecurity behaviors of university students, particularly in emerging regions like Albania, is crucial in today's digital age. As highlighted by Hong et al. (2023), factors such as education levels and work exposure significantly shape cybersecurity practices, underscoring the need for tailored interventions (Hong, et al., 2023). As cybersecurity threats evolve rapidly, traditional defenses are no longer enough, and proactive strategies are critical to mitigate risks and maintain digital safety (Raya, Yahya, & Ahmad, 2023; Kuraku, Kalla, Samaah, & Smith, 2023).

University students represent both a vulnerable demographic and future leaders in digital security, with their online behaviors impacting personal and organizational safety. While Albanian students increasingly use the internet (INSTAT, 2023), gaps remain in advanced cybersecurity practices, such as password management and phishing detection. This study investigates these gaps, highlighting the disconnect between students' threat awareness and actual behaviors, a critical issue for regions undergoing digital transformations.

This research aims to explore students' cybersecurity practices and perceptions in Albania, with the goal of identifying the specific vulnerabilities they face.

To address these issues, the study is guided by the following research questions:

- What cybersecurity practices do students use to protect their personal information online?
- What are students' perceptions of cybersecurity risks?
- How do students respond to perceived cybersecurity threats?

By addressing these gaps, the study seeks to contribute insights into the broader conversation on cybersecurity in developing nations, emphasizing the importance of regionally tailored educational interventions.

## 1. LITERATURE REVIEW

Cybersecurity awareness is critical in fostering secure online behavior, particularly among students, a vulnerable group in the digital age (Chaudhary, 2024). Muniandy et al. (2017) critically analyzed cybersecurity behaviors among Malaysian university students, revealing significant deficiencies in both awareness and secure practices. Their findings highlighted that students often neglect advanced security measures, such as phishing recognition and effective password management. This underscores the need for targeted interventions. Such insights are especially useful for understanding the challenges in underrepresented contexts like Albania, where cultural, educational, and technological factors may shape students' cybersecurity behaviors in unique ways. Moallem (2019) observed a similar disparity in Silicon Valley, where students' theoretical knowledge of cybersecurity risks did not translate into effective practices. While students understood risks like surveillance and hacking, their practical skills in safeguarding data were limited.

Behavioral theories provide important frameworks for understanding the cognitive and motivational factors that influence cybersecurity behaviors. Mashiane and Kritzinger (2019) developed a taxonomy categorizing cybersecurity behaviors into awareness, prevention, and response. This taxonomy can help shape interventions that focus on recognizing phishing attempts, improving password management, and encouraging the timely reporting of incidents.

Password management remains a major cybersecurity challenge (Temoshok, et al., 2024) for students. Shay et al. (2014) found that simplifying password creation rules—such as reducing character constraints—can improve both usability and security. Li, Wang, and Sun (2016) further identified vulnerabilities in common password habits, particularly the use of easily guessable personal information, underscoring the importance of password hygiene training. Educating students about the dangers of reusing passwords and embedding personal details can help reduce the risk of credential-based attacks. Li and Zeng (2021) examined the use of Leet speech (e.g., replacing "e" with "3") in passwords, demonstrating that less common Leet variations can significantly improve password strength. Wang, Salehi-Abari, and Thorpe (2023) introduced PiXi, a gamified framework designed to motivate users to create stronger passwords, offering a promising approach for educational settings.

To address these challenges, universities should adopt a multifaceted approach, emphasizing proactive rather than reactive measures in password management. By addressing the factors influencing password choices, universities can play a key role in fostering long-term behavioral change and reducing the risks associated with poor password hygiene (Temoshok, et al., 2024).

Students' perceptions of cybersecurity threats play a crucial role in shaping their responses to risks. Research by Zwilling et al. (2022) reveals a significant gap in student awareness, as they tend to recognize high-profile threats like malware but underestimate subtler risks such as phishing, adware, and social engineering. This discrepancy highlights the need for targeted interventions focused on these overlooked threats. Chandarman and Van Niekerk (2017) found that customized interventions, such as phishing simulations, significantly reduce risky behaviors. This suggests a need for experiential learning approaches, such as interactive cybersecurity labs or real-time threat simulations, to bridge the gap between theoretical knowledge and practical application.

DOI: <https://doi.org/10.29352/mill0227.41111>

1.1 Global and Regional Cybersecurity Trends

Globally, phishing and compromised credentials continue to dominate as the most common attack vectors, with ransomware incidents increasing by 19.5% in 2023 (IBM, 2023). The average cost of a data breach reached a record high of \$4.45 million, with the United States leading globally at \$9.48 million per breach. These trends underscore the growing sophistication of cyber threats and the urgent need to equip vulnerable populations, such as students, with robust cybersecurity practices to mitigate risks. The healthcare sector, particularly in the United States, remains the most affected, with the average cost of a breach reaching \$10.93 million, an increase of 8.2% compared to 2022 (IBM, 2023).

Within the European Union (EU), the landscape of cybersecurity incidents reveals disparities in organizational preparedness and response. According to Eurostat (2022), 22% of EU companies experienced cybersecurity issues, with Finland (44%), the Netherlands (30%), and Poland (30%) reporting the highest rates. Conversely, countries such as Portugal (12%), Slovakia (12%), and Bulgaria (11%) reported fewer incidents, reflecting varying levels of readiness and investment in cybersecurity measures. Figure 1 illustrates data from the European Union Agency for Cybersecurity (ENISA) (European Union Agency for Cybersecurity, 2024), categorizing 4,567 cyber incidents between 2012 and 2024 into system failures (56%), malicious actions (24%), human errors (16%), and natural phenomena (4%). The dominance of system failures emphasizes the critical importance of system maintenance and regular updates to prevent disruptions. Malicious actions, including phishing and malware attacks, account for nearly a quarter of incidents, underscoring the necessity for investment in preventive measures and cybersecurity awareness campaigns (Mattioli & Malatras, 2024). Human errors rank third, highlighting the need for training programs to mitigate mistakes that compromise security.

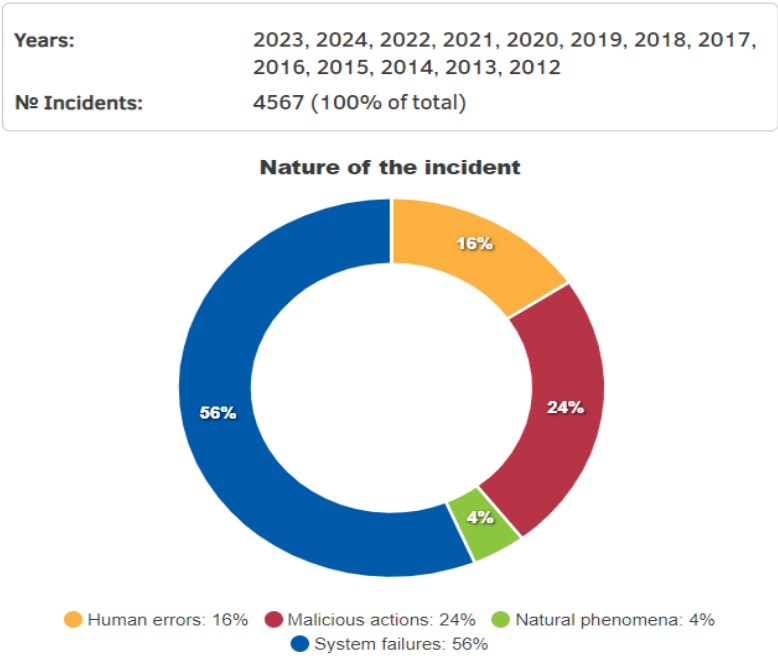
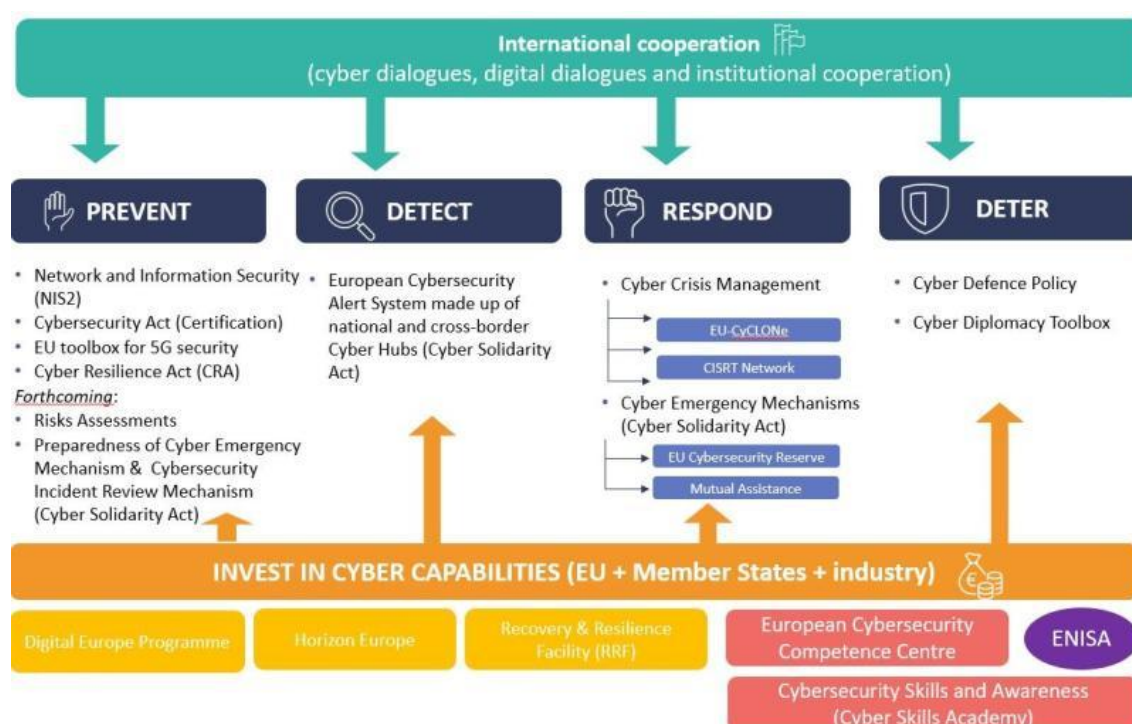


Figure 1 - Nature of Cyber Incidents (2012–2024)  
Source: (European Union Agency for Cybersecurity, 2024)

The EU’s cybersecurity strategy, shown in Figure 2, is built around four pillars: prevention, detection, response, and deterrence. Prevention focuses on frameworks such as the Cybersecurity Act and risk assessments, while detection relies on cross-border cooperation through tools like the European Cybersecurity Alert System. Response mechanisms include initiatives like Cyber Crisis Management and the Cyber Solidarity Act, enabling swift reactions to cyber incidents. The EU also invests heavily in building cyber capabilities through initiatives such as the European Cybersecurity Competence Centre and the Cyber Skills Academy, which emphasize the importance of cybersecurity awareness and education (European Commission, 2024).

DOI: <https://doi.org/10.29352/mill0227.41111>



**Figure 2 - EU Strategy for Cybersecurity**  
Source: (European Commission, 2024)

## 1.2 Albania's Cybersecurity Landscape

Albania's rapid digital transformation presents both opportunities and challenges for its cybersecurity landscape. With 83.1% of the population aged 16–74 actively using the internet (INSTAT, 2023), the nation is experiencing unprecedented connectivity. However, this surge in digital activity has also heightened vulnerabilities, particularly among students who represent a critical yet underexplored demographic. Students' reliance on digital platforms for education, communication, and financial transactions increases their exposure to sophisticated cyber threats, including phishing, ransomware, and social engineering (National Authority for Electronic Certification and Cyber Security, 2023). The National Authority for Electronic Certification and Cybersecurity (2023) highlights that the banking sector (36%) and digital infrastructure (31%) are the most targeted sectors for cyber incidents in Albania. Despite the growing prevalence of cyber threats, Albania remains underrepresented in global cybersecurity research. This study seeks to bridge this gap by focusing on the cybersecurity behaviors and perceptions of Albanian students, a demographic that has received limited academic attention but plays a crucial role in shaping the country's digital future. Understanding how students perceive and respond to threats such as phishing and ransomware is essential for crafting targeted interventions and educational programs. By examining a population that serves as both individual users and future professionals, this study highlights the critical role of student cybersecurity habits in shaping Albania's growing digital economy. Addressing this gap offers actionable insights for strengthening national cybersecurity strategies and contributing to global initiatives aimed at fostering secure online behaviors in emerging digital societies.

Building on the insights from the global and regional cybersecurity trends outlined above, this study investigates the unique challenges faced by Albanian students and is guided by the following hypothesis:

H1: Students who exhibit proactive cybersecurity behaviors, such as frequently updating antivirus software, are significantly less likely to experience or report malware-related incidents (e.g., viruses, adware, spyware) than those who engage in less frequent software updates.

## 2. METHODS

This study employs a quantitative approach to investigate the cybersecurity behaviors, perceptions, and responses of university students in Albania. The research integrates established cybersecurity behavior frameworks to collect data on students' digital security practices, threat awareness, and incident response behaviors.



DOI: <https://doi.org/10.29352/mill0227.41111>

## 2.1 Sample

The study involved 242 university students from various IT-related disciplines, including Information Technology, Computer Engineering, Business Informatics, and Applied Informatics. This study focuses on IT-related students due to their critical role in shaping cybersecurity practices, both academically and professionally. Their behaviors and perceptions are crucial for understanding regional and global cybersecurity strategies. The demographic breakdown of the sample is as follows: 59.9% male (145) and 40.1% female (97), with 51% of participants employed, representing a mix of full-time students and working individuals.

## 2.2 Data collection instruments

The survey instrument was developed based on a review of the literature on cybersecurity behaviors and perceptions (Chaudhary, 2024; Chandarman & Van Niekerk, 2017; Zwilling, et al., 2022; Mashiane & Kritzinger, 2019; Li & Zeng, 2021). It consists of three key sections:

- Demographic Information.
- Cybersecurity Practices: Assesses behaviors like antivirus use, password management, and phishing detection.
- Cybersecurity Perceptions: Uses a 5-point Likert scale to measure students' awareness of cybersecurity risks and confidence in protective measures.

The survey was distributed online between March and May 2024. Participants were informed of the study's objectives, and informed consent was obtained before their participation, ensuring compliance with ethical standards. The anonymity and confidentiality of respondents were maintained throughout the study. The study provides a snapshot of students' cybersecurity behaviors at one point in time and does not capture long-term trends or the effects of educational interventions over time. Future research could examine longitudinal changes in cybersecurity behaviors. The study focuses on Albania, a country underrepresented in global cybersecurity research. Comparative studies across regions could provide deeper insights into how different cultural, educational, and infrastructural factors influence cybersecurity behaviors.

## 2.3 Statistical analysis

The data collected in this study were analyzed using JASP 0.18.3.0, a statistical software that offers a wide range of analytical tools. To examine the relationship between proactive cybersecurity behaviors and the likelihood of encountering or reporting cybersecurity incidents, a logistic regression analysis was conducted. This method was chosen because it is well-suited for predicting binary outcomes, such as whether or not students experience or report malware-related incidents, based on independent variables like cybersecurity practices. The coefficients for the proactive cybersecurity behaviors were calculated to determine the odds of students experiencing or reporting malware-related incidents. Additionally, Cronbach's alpha was calculated to assess the internal consistency of the survey instrument. The reliability coefficient was found to be 0.913, which indicates strong internal consistency, exceeding the acceptable threshold of 0.7, confirming that the survey items reliably measured the intended constructs of cybersecurity behaviors and perceptions.

## 3. RESULTS

What cybersecurity practices do students use to protect their personal information online?

The study's analysis of students' cybersecurity practices demonstrates solid engagement with fundamental protective measures, yet there are critical gaps in advanced security behaviors (Table 1). A significant 89.67% of students reported having antivirus software installed, with 65.70% ensuring automatic updates. Moreover, 75.62% of students reported enabling firewalls, indicating an understanding of basic security protocols. However, in the area of password management, a notable vulnerability was identified. While 45.04% of students used unique passwords for each account, 19.01% stored passwords in the cloud, and 18.60% wrote them down on paper, which significantly increases their exposure to cyberattacks. Additionally, 82.6% of students used public Wi-Fi, with many likely using VPNs to mitigate the associated risks.

Phishing detection was another area where a knowledge gap was evident: 65.70% of students reported being able to recognize phishing attempts, yet 34.30% still lacked awareness of such risks. This indicates that despite the widespread use of basic security tools, there is a gap in more sophisticated areas of cybersecurity awareness and protection.

DOI: <https://doi.org/10.29352/mill0227.41111>

**Table 1 - Users' cybersecurity practices**

	Cybersecurity Practices			Frequency	Percent
Cybersecurity Practices	Antivirus software installation and update frequency	Antivirus software installation	No	19	7.85
			I do not know	6	2.48
			Yes	217	89.67
			Total	242	100
		Antivirus Update Frequency	Never	18	7.44
			Manual Updates (e.g., twice a week)	7	2.89
			Manual Updates (e.g., subscription ends)	27	11.16
			Manual Updates (e.g., once a week)	10	4.13
			Manual Updates (e.g., once a month)	21	8.68
			Automatic Updates	159	65.70
			Total	242	100
	Firewall Usage	Firewall Installation	Not Enabled	33	13.64
			Unsure	26	10.74
			Enabled	183	75.62
			Total	242	100
	Public Wi-Fi Usage	Use of open Wi-Fi in public places.	No	42	17.4
			Yes	200	82.6
			Total	242	100
	Awareness of Phishing	Phishing detection.	Cannot Identify	83	34.30
			Can Identify	159	65.70
			Total	242	100
	Password Management	Number of passwords.	Alternating Passwords Between Accounts	110	45.46
			Same Password for All Accounts	23	9.50
			Unique Passwords for Each Account	109	45.04
			Total	242	100
		Use of password managers.	No	152	62.81
			Yes	90	37.19
			Total	242	100
		Password memorability.	I keep them in the cloud	46	19.01
			I keep them in a folder on my computer	47	19.42
			I save them in the browser	15	6.20
			I write them on paper	45	18.60
			I do not remember them	18	7.44
			Use a password manager	44	18.18
			Use only 1	27	11.16
			Total	242	100

What are students' perceptions of cybersecurity risks?

The students demonstrated moderate to high concern regarding cybersecurity threats (Table 2), as reflected in their perceptions of internet security (mean score: 3.736) and the security of online shopping and banking (mean score: 3.607). Concerns about viruses (mean: 4.289) and hackers (mean: 4.231) were notably high, which aligns with students' proactive behaviors like installing antivirus software and enabling firewalls. However, less concern was shown for threats such as adware (mean: 3.202) and phishing (mean: 3.186), suggesting a lack of awareness regarding these increasingly sophisticated threats. This finding underscores the need for targeted educational initiatives focused on phishing, adware, and other subtle but potentially damaging risks.

**Table 2 - Threat perceptions**

		Valid	Mean	95% Confidence Interval Mean		Minimum	Maximum
				Upper	Lower		
Threat Perceptions	Internet Security Concerns	242	3.736	3.877	3.594	1	5
	Online Shopping and Banking Security Concerns	242	3.607	3.765	3.45	1	5
	Computer virus	242	4.289	4.39	4.188	1	5
	Adware	242	3.202	3.363	3.042	1	5
	Spyware	242	3.343	3.511	3.175	1	5
	Phishing	242	3.186	3.368	3.004	1	5
	Hacker	242	4.231	4.354	4.108	1	5
	Firewall	242	4.025	4.167	3.883	1	5
	Identity theft	242	3.628	3.794	3.462	1	5
	Worm	242	3.194	3.362	3.026	1	5
	Trojan horse	242	3.463	3.645	3.281	1	5
	Concern levels for various cybersecurity threats	242	3.186	3.368	3.004	1	5

DOI: <https://doi.org/10.29352/mill0227.41111>

### How do students respond to perceived cybersecurity threats?

When it comes to responding to cybersecurity threats, students were significantly more likely to report security breaches when anonymity was assured (Table 3). In personal online environments, 83.88% of students stated they would report a breach if anonymity were guaranteed. This figure increased slightly for breaches in academic or professional contexts (86.78%) under similar conditions. However, reporting likelihood dropped to 80.99% in personal contexts and 81.82% in academic/professional contexts when anonymity was not promised.

Moreover, exposure to previous cybersecurity breaches had a noticeable effect on students' online behavior: 79.75% of students indicated they had modified their online behaviors after experiencing a security incident. This shows that personal exposure to cyber threats can encourage proactive changes in cybersecurity habits.

**Table 3 - Behavioral Responses**

Behavioral Responses			Frequency	Percent	
Behavioral Responses	Reporting Security Breaches	Would you report a security breach in your personal online environment if anonymity was maintained?	No	39	16.116
			Yes	203	83.884
			Total	242	100
		Would you report a security breach in your personal online environment if anonymity was not maintained?	No	46	19.008
			Yes	196	80.992
			Total	242	100
		Would you report a security breach in your professional or academic context if anonymity was maintained?	No	32	13.223
			Yes	210	86.777
			Total	242	100
	Would you report a security breach in your professional or academic context if anonymity was not maintained?	No	44	18.182	
		Yes	198	81.818	
		Total	242	100	
Actions Following Security Breaches	Have you ever changed your online behavior after a security breach	No	49	20.248	
		Yes	193	79.752	
		Total	242	100	

H1: Students who exhibit proactive cybersecurity behaviors, such as frequently updating antivirus software, are significantly less likely to experience or report malware-related incidents (e.g., viruses, adware, spyware) than those who engage in less frequent software updates.

The results of the logistic regression analysis (Table 4) provide compelling support for H1, indicating that students who engage in proactive cybersecurity behaviors, such as frequent antivirus updates, are significantly less likely to experience or report malware-related incidents. The comparison between the null model ( $M_0$ ) and the model with proactive cybersecurity behaviors ( $M_1$ ) reveals a substantial improvement in model fit, underscoring the importance of these behaviors in predicting digital security outcomes. Despite the modest McFadden's  $R^2$ , the statistical significance of the model improvement ( $\Delta X^2 = 16.176$ ,  $p < .001$ ) suggests that even small behavioral changes can have a meaningful impact on reducing malware risks. The model reveals a substantial reduction in the likelihood of infection, with an odds ratio of 0.138, reflecting an 86.2% decrease in the odds of malware infections for students who adopt these cybersecurity practices (Table 5). This underscores the critical role that proactive behaviors play in mitigating cyber risks, particularly in a rapidly evolving digital landscape where students are increasingly vulnerable to sophisticated cyber threats.

The model demonstrates exceptional predictive accuracy, with accuracy at 92.1%. The high precision (0.917) and F-measure (0.957) further emphasize that the model achieves an optimal balance between correctly identifying true positives (malware infections) and minimizing false positives, highlighting its robustness in identifying at-risk students. These findings strongly reinforce the importance of fostering proactive cybersecurity practices within university settings.

**Table 4 - Logistic Regression**

Model Summary -Predicting Malware-Related Incidents Based on Proactive Cybersecurity Behaviors									
Model	Deviance	AIC	BIC	df	$\Delta X^2$	p	McFadden $R^2$	Nagelkerke $R^2$	Tjur $R^2$
$M_0$	189.054	191.054	194.543	241			0		0
$M_1$	172.878	176.878	183.856	240	16.176	< .001	0.086	0.119	0.146

Note.  $M_1$  includes proactive cybersecurity behaviors

**Table 5 - Coefficients**

Model		Estimate	Odds Ratio	p
$M_0$	(Intercept)	1.881	6.562	< .001
$M_1$	(Intercept)	5.897	363.939	< .001
	Proactive cybersecurity behaviors	-1.98	0.138	< .001



DOI: <https://doi.org/10.29352/mill0227.41111>

#### 4. DISCUSSION

This study provides valuable insights into the cybersecurity practices and perceptions of university students in Albania, a region experiencing rapid digital engagement. The findings align with previous research that highlights the increasing cybersecurity challenges faced by students (Chaudhary, 2024; Muniandy, Muniandy, & Samsudin, 2017). While students demonstrate a basic understanding of fundamental security practices, critical gaps remain in more advanced areas, such as password management and phishing detection. These vulnerabilities are not unique to Albania, as similar issues have been identified globally, emphasizing the urgent need for comprehensive cybersecurity education (Hong, et al., 2023; Mashiane & Kritzinger, 2019).

Students' engagement with essential cybersecurity measures, such as antivirus software installation (89.67%) and firewall usage (75.62%), indicates a foundational understanding of digital security (Chaudhary, 2024; Temoshok, et al., 2024). However, significant gaps remain in more advanced practices, such as phishing detection and secure password management. This aligns with the findings of Muniandy et al. (2017), who highlighted that students often neglect these critical areas. Zwilling et al. (2022) also pointed out that while students recognize prominent threats like malware, they often overlook subtler risks, such as phishing and adware. This discrepancy between awareness and actual behavior suggests a reactive rather than proactive approach to cybersecurity, underscoring the need for targeted interventions.

A key finding of this study is that students are more likely to report cybersecurity incidents when anonymity is assured. This is consistent with Chandarman and Van Niekerk (2017), who found that anonymous reporting mechanisms enhance reporting rates, thereby improving cybersecurity incident management. By implementing anonymous reporting systems, universities can foster a more open and proactive cybersecurity culture, encouraging students to report incidents without fear of personal or professional consequences.

The logistic regression analysis supports the hypothesis that proactive cybersecurity behaviors, such as frequent antivirus updates, are linked to a reduced likelihood of experiencing or reporting malware-related incidents. These findings are in line with Li et al. (2016) and Li & Zeng (2021), who emphasized the importance of proactive measures in strengthening digital security. The model's high predictive accuracy (92.1%) further confirms the effectiveness of these practices in reducing the likelihood of malware infections.

The study's results suggest that universities should prioritize educational interventions focusing on advancing students' cybersecurity skills, particularly in areas such as phishing detection and password management. Following recommendations from Chaudhary (2024) and Mashiane & Kritzinger (2019), universities should incorporate practical, hands-on cybersecurity training, including real-time simulations and interactive labs, to bridge the gap between theoretical knowledge and real-world application. Additionally, the study found that personal experiences with cyber threats significantly influence students' cybersecurity behaviors. This aligns with Muniandy et al. (2017), who noted that exposure to cybersecurity incidents motivates students to adopt better security practices. Universities should design interventions that simulate realistic cyber threat scenarios to enhance students' practical awareness and preparedness for future incidents.

Recommendations for Future Research and Institutional Action:

1. Extended Research: Future studies should investigate other essential cybersecurity behaviors, such as firewall usage and secure browsing practices, to further understand students' digital security habits.
2. Longitudinal Studies: Long-term research is needed to examine how students' cybersecurity practices evolve over time, particularly in response to educational interventions.
3. Institutional Actions: Universities should integrate proactive cybersecurity education into their curricula, focusing on practical skills, incident response, and raising awareness of emerging threats, such as phishing and social engineering.

#### CONCLUSION

This study identifies critical vulnerabilities in cybersecurity practices among university students in Albania, underscoring the urgent need for enhanced proactive and practical cybersecurity education. Our findings, consistent with global cybersecurity trends, reveal substantial gaps, particularly in sophisticated protective behaviors like phishing detection and secure password management.

A key contribution of this study is its empirical demonstration that proactive behaviors, notably regular antivirus updates, markedly reduce malware-related incidents. Logistic regression analysis provided rigorous methodological support, clearly connecting these proactive cybersecurity behaviors with improved security outcomes.

Additionally, the research highlights the pivotal role of anonymous reporting mechanisms, significantly increasing students' willingness to report cybersecurity incidents. This finding underscores the necessity for universities to implement privacy-preserving reporting practices. The study's methodological strengths, including its robust analytical framework and comprehensive approach integrating behavioral, perceptual, and contextual insights, significantly enrich the literature by providing targeted educational strategies for enhancing digital security.

Future research should extend these findings through longitudinal studies assessing sustained behavioral changes, comparative analyses across various educational settings, and expanded exploration of behaviors such as VPN usage and multi-factor authentication.

In conclusion, the practical implications derived from this research are substantial, advocating evidence-based curricular and policy interventions that cultivate resilient cybersecurity cultures. Ultimately, strengthening cybersecurity education at universities not only safeguards students but also contributes significantly to broader societal resilience in the increasingly complex digital landscape.

DOI: <https://doi.org/10.29352/mill0227.41111>

## AUTHORS' CONTRIBUTION

Conceptualization, A.F., F.M., R.S. and A.O.; data curation, A.F. and F.M.; formal analysis, A.F., F.M. and R.S.; investigation, A.F.; methodology, A.F., F.M., R.S. and A.O.; project administration, A.F. and F.M.; resources, A.F., F.M., R.S. and A.O.; software, A.F.; supervision, A.F.; validation, A.F., F.M., R.S. and A.O.; writing-original draft, A.F.; writing-review and editing, A.F., F.M., R.S. and A.O.

## CONFLICT OF INTEREST

The authors declare no conflict of interest.

## REFERENCES

- Albanian Institute of Statistics (INSTAT). (2023). *Use of Information and Communication Technology in the Household, 2023*. <https://www.instat.gov.al/media/11339/use-of-ict-in-households-2023.pdf>
- Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication (AJIC)*, 20, 133–155. <https://doi.org/10.23962/10539/23572>
- Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, 142, Article 103858. <https://doi.org/10.1016/j.cose.2024.103858>
- European Commission. (2024, April 29). *Policies: European Commission*. Retrieved June 5, 2024. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity>
- European Union Agency for Cybersecurity. (2024, June 29). *Incident reporting: ENISA*. <https://ciras.enisa.europa.eu/>
- Eurostat. (2022, December). *Statistical themes: Eurostat*. [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT\\_security\\_in\\_enterprises#ICT\\_security\\_in\\_EU\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises)
- Hong, W. C., Chi, C., Liu, J., Zhang, Y., Lei, V. N., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Education and Information Technologies*, 28(1), 439–470. <https://doi.org/10.1007/s10639-022-11121-5>
- IBM. (2023). *Cost of a data breach report 2023*. <https://www.ibm.com/reports/data-breach>
- Kuraku, S., Kalla, D., Samaah, F., & Smith, N. (2023). Cultivating proactive cybersecurity culture among IT professionals to combat evolving threats. *International Journal of Electrical, Electronics and Computers (IJEEC)*, 8(6), 1–7.
- Li, W., & Zeng, J. (2021). Leet usage and its effect on password security. *IEEE Transactions on Information Forensics and Security*, 16, 2130–2143. <https://doi.org/10.1109/TIFS.2021.3050066>
- Li, Y., Wang, H., & Sun, K. (2016). A study of personal information in human-chosen passwords and its security implications. *IEEE INFOCOM 2016 – The 35th Annual IEEE International Conference on Computer Communications* (pp. 1–9). IEEE. <https://doi.org/10.1109/INFOCOM.2016.7524341>
- Mashiane, T., & Kritzing, E. (2019). Cybersecurity behaviour: A conceptual taxonomy. In O. Blazy & C. Yeun (Eds.), *Information Security Theory and Practice (WISTP 2018)* (Vol. 11469, pp. 147–156). Springer. [https://doi.org/10.1007/978-3-030-20074-9\\_11](https://doi.org/10.1007/978-3-030-20074-9_11)
- Mattioli, R., & Malatras, A. (2024). *Incident reporting: ENISA*. European Union Agency for Cybersecurity (ENISA). <https://abrir.link/BPZwm>
- Moallem, A. (2019). Cybersecurity awareness among college students. In T. N. Ahram (Ed.), *Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing* (Vol. 782, pp. 79–87). Springer. [https://doi.org/10.1007/978-3-319-94709-9\\_8](https://doi.org/10.1007/978-3-319-94709-9_8)
- Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity*, 2017, Article 800299. <https://doi.org/10.5171/2017.800299>
- National Authority for Electronic Certification and Cyber Security. (2023). *Cyber governance 2023 report*. Tirana, Albania: Author.
- Raya, J. E., Yahya, A. S., & Ahmad, E. K. (2023). Protection from a quantum computer cyber-attack: Survey. *Technium: Romanian Journal of Applied Sciences and Technology*, 5, 1–12. <http://dx.doi.org/10.47577/technium.v5i.8293>
- Shay, R., Komanduri, S., Durity, A. L., Huh, P., Mazurek, M. L., Segreti, S. M., Ur, B., Bauer, L., Christin, N., & Cranor, L. F. (2014). *Can long passwords be secure and usable? CHI '14: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2927–2936). Association for Computing Machinery. <https://doi.org/10.1145/2556288.2557224>
- Temoshok, D., Fenton, J. L., Choong, Y.-Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R., & Richer, J. P. (2024). *NIST SP 800-63B-4.2pd: Digital identity guidelines: Authentication and authenticator management (Second Public Draft)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-63b-4.2pd>
- Wang, S., Salehi-Abari, A., & Thorpe, J. (2023). PiXi: Password inspiration by exploring information. *Information and Communications Security: 25th International Conference, ICICS 2023* (pp. 249–266). Springer. [https://doi.org/10.1007/978-3-031-44698-8\\_14](https://doi.org/10.1007/978-3-031-44698-8_14)
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82–97. <https://doi.org/10.1080/08874417.2020.1712269>