Digitally Embodied Self and Online Safety Practices Among Young Albanian Net Users: A Quantitative Study of Risk Behaviors and Privacy Perceptions

DOLANTINA HYKA [1], FATMIR BASHOLLI [2], FESTIM KODRA [3]

[1] Department of Information Technology, [2] Department of Engineering, [3]Department of Finance, Bank and Accounting
[1,3]Mediterranean University of Albania, [2] European University of Tirana
Address: [1,3]Gjergj Fishta, Nr. 52, 1023 Tirana, [2] Xhura Complex, St. Xhanfize Keko, Tirana
[1,2,3]ALBANIA

Abstract: This study examines digital awareness and online safety practices among Albanian youth, focusing on risky behaviors and perceptions of privacy. Using a quantitative questionnaire completed by 120 participants aged 15–25, the research analyzed internet usage habits, knowledge of protective measures, experiences with online harassment, and reactions to such situations. Findings reveal a gap between awareness and action, with low adoption of security practices such as two-factor authentication. Gender and age differences in digital awareness and behavior were also observed. The study highlights the urgent need for educational programs and policy interventions to strengthen digital safety and awareness in Albania.

Key-Words: - Digital awareness; Online security; Privacy; Youth; Risky behaviors; Albania

Received: May 23, 2025. Revised: June 29, 2025. Accepted: September 17, 2025. Published: October 22, 2025.

1 Introduction

In an era where nearly all information is exchanged online through various platforms such as websites, social media, and other digital channels, young people represent one of the most active groups in the use of digital technologies. The internet and social media platforms have become integral parts of their daily lives, offering numerous opportunities but also exposing them to a wide range of risks. [1] Unlimited access to content, communication with strangers, sharing personal information, and exposure to online harassment are among the most pressing challenges associated with youth behavior online[2].

In the Albanian context, where digital safety education remains limited within school curricula and awareness is more individual than institutional, there is a growing need to assess the current state of knowledge, behaviors, and perceptions that young people hold regarding online safety and privacy.

This study aims to explore:
• the level of digital awareness among young people;
• their common behaviors related to online privacy;
•their experiences with online threats and risky situations;
• and how the Albanian youth cope with these challenges.

Using a structured questionnaire, data were collected from over 100 participants aged 15 to 25 across various regions in Albania. The findings will be analyzed to identify links between demographic factors (such as age and gender) and risky online behaviors, as well as to uncover potential gaps in knowledge and awareness.

This paper seeks to contribute to both national and international literature on digital education and aims to serve as a foundation for structured educational

interventions and the development of youth protection policies in the digital environment.

2 Problem Formulation

The widespread use of the internet among young people has been accompanied by a growing exposure to cyber risks, including online bullying, unsafe social networks, digital scams, and violations of personal privacy [1]. Previous research has shown that awareness of online dangers does not always align with actual behavior. Many young users report having basic knowledge about online privacy, yet they continue to share personal information in uncontrolled ways. This disconnect highlights the need to measure not only knowledge, but also the attitudes and concrete practices of young people regarding digital safety [3].

In Albania, research on online safety among youth remains limited. Partial reports from international organizations such as UNICEF and Save the Children have emphasized the presence of digital bullying and the lack of systematic education on the safe use of technology [4], [5]. However, standardized quantitative studies analyzing the actual behaviors and perceptions of Albanian youth regarding data protection and digital interaction are still lacking.

From a theoretical perspective, this area of study is supported by models such as the Theory of Planned Behavior [6] and the Protection Motivation Theory [7], which explain that safety-related behaviors are influenced by perceived risk, self-efficacy, and potential benefits. These models have been widely applied to understand decision-making in information security contexts [8].

More recent studies on youth across the Balkan region reveal an alarming trend: heavy overlap between social media use and high exposure to inappropriate content, interactions with strangers, and uncontrolled sharing of personal information [9]. These findings reinforce the need for localized research that assesses approaches to online safety within the social and cultural context of countries like Albania, where digital education is still in development.

This study, based on a structured and online-distributed questionnaire, aims to fill this gap by offering a detailed overview of:

• the online behaviors of Albanian youth,

•their perceptions of digital risks and personal privacy,

• and the relationship between knowledge, attitudes, and actual behaviors in response to online threats.

It contributes to the existing literature by providing new data that can support the design of educational policies, raise community awareness, and inform the development of customized training programs at both the school and national levels.

This study employed a quantitative-descriptive approach aimed at assessing the level of digital awareness and online safety practices among Albanian youth. Data were collected through an electronic questionnaire composed of several core sections covering demographic information, internet usage habits, knowledge of security measures, and experiences and perceptions related to online risks.

The survey was developed using Google Forms and was distributed digitally through social media platforms and community groups to capture a diverse range of participants from different cities across Albania. A total of 120 young people, aged between 15 and 25, took part voluntarily and anonymously in this survey.

We developed a concise survey combining multiple-choice items, Likert- scale statements, and targeted open prompts, then pilot-tested it with ten students to ensure clarity. After confirming internal consistency (Cronbach's $\alpha = 0.78$), we administered it to 120 Albanian youths aged 15–25. Responses were first cleaned and tabulated in Excel before being imported into SPSS. We used the means and frequencies to sketch participants' digital habits, and medians with interquartile ranges to respect the ordinal nature of Likert items. Cross- tabulations and Chi- Square tests ($\alpha = 0.05$) then explored associations between age, gender, and safety behaviors. All analyses adhered to ethical standards: each respondent provided informed consent, and our protocol received approval from the university's review board. This approach yielded not just numbers, but a nuanced narrative of how awareness, perception, and behavior intertwine in young Albanians' online lives.

3 Problem Solution

In interviewing young Albanians about their online habits, two clear weaknesses emerged. First, despite easy access to security tools, only 27 % of participants had ever enabled two-factor authentication. This low uptake leaves most accounts exposed to simple hacks or phishing attempts. Second, fewer than half, just 42 %, used a unique password for each service. Reusing credentials across multiple sites turns a single breach into a cascade of compromises.

These patterns reveal more than mere forgetfulness. They point to a lack of practical, hands-on experience with digital safety. Knowing that 2FA exists and

setting it up are very different skills. Likewise, creating and managing separate passwords requires concrete habits, not just abstract awareness.

To close these gaps, we recommend: Embedding digital hygiene lessons into school curricula, so students learn by doing, installing 2FA, crafting strong, unique passwords, and using password managers.

Offering interactive workshops and simulations, where teens practice protecting a mock account against real-world attack scenarios.[10]

By moving from passive awareness to active skill-building, we can help Albanian youth turn knowledge into habits and significantly strengthen their online defenses.

Key Issue	**Statistics / Findings**	**Analysis / Explanation**	**Recommendations**
Limited implementation of basic security measures	Only 27% have activated 2FA	Low usage despite the availability of tools	Practical training and active digital safety interventions
Use of different passwords for different accounts	Only 42% use distinct passwords	High vulnerability in account protection	Embed digital hygiene lessons into school curricula
Reason for low numbers	Lack of routine exposure to digital hygiene	Passive awareness is insufficient	Classroom modules, workshops, and peer-led exercises

Table 1: Digital Safety Gap Analysis & Recommendations. (by authors)

These low numbers are indicative not merely of negligence, but of a lack of routine exposure to digital hygiene practices within structured educational or social settings. This calls for a shift from passive awareness campaigns to active, hands-on digital safety instruction. Such instruction should be embedded into the formal education system through classroom-based modules, workshops, and peer-led exercises that foster experiential learning.

Another area of concern is the low rate of action in response to negative digital experiences. While over half of the respondents stated that they were familiar with how to report online harassment or abuse, fewer than one in five had ever done so. This discrepancy suggests not only a lack of confidence in reporting mechanisms but also an internalization of digital harassment as something normal or unworthy of attention.

Familiar with Reporting Mechanisms	**Percentage (%)**	**Have Reported Harassment (%)**
Yes	55%	18%

Table. 2: Awareness vs. actual reporting of online harassment. (by authors)

Many young people may not recognize certain interactions as dangerous or may perceive reporting as futile due to institutional inaction. Thus, the solution here lies both in reinforcing awareness about what constitutes digital abuse and in improving institutional responsiveness. Youth need to be reassured that their complaints will be taken seriously and that there are clear, accessible, and youth-friendly channels through which they can seek help.

The data also revealed notable gender differences. Female participants generally exhibited more cautious and privacy-conscious behavior online, being more likely to use security measures and more attentive to personal boundaries. Male participants, in contrast, were less likely to adopt protective practices or to express concern about digital risks. These findings point to the importance of gender-responsive interventions. Programs aimed at boys should actively challenge attitudes of digital invulnerability and encourage more critical thinking about long-term consequences. Meanwhile, programs for girls may benefit from focusing on empowerment, reinforcing the legitimacy of asserting digital boundaries and seeking support when needed.

Younger teens (15-18) show less online risk perception than older youth (19-25). This is alarming. Younger users are often more vulnerable online due to inexperience. A lack of formal digital education exacerbates this [11]. They face higher risks of exploitation. Therefore, early digital risk education is crucial. This instruction must be age-appropriate. It should use storytelling, real-life scenarios, and simulations. These methods can effectively show how digital risks appear and how to manage them.

Systemically, Albanian schools lack consistent digital safety education. Digital literacy often focuses only on technical skills. It neglects ethics, privacy rights, and cyber defense. This creates a significant

gap. Digital citizenship topics need formal integration into national curricula. Teachers require tools and training to deliver this content well. Without institutional backing, current educational efforts will remain fragmented.

Culturally, one of the most persistent problems is the normalization of risky online behavior. Young people frequently share personal information online without considering the consequences, communicate freely with strangers, and minimize the seriousness of online harassment. These behaviors are shaped not only by a lack of knowledge but also by peer influence, social media trends, and the absence of strong digital role models [12]. A long-term solution requires a cultural shift—one that encourages critical engagement with digital environments, promotes personal responsibility, and values privacy as a collective right, not just an individual preference.

Taken together, these findings suggest that digital safety cannot be achieved through isolated interventions or one-off awareness campaigns. Rather, it requires a sustained, age-appropriate, and socially embedded educational strategy, one that involves schools, families, communities, and policy institutions [13], [14]. Only through such an integrated approach can we expect to see meaningful improvements in how young Albanians navigate the digital world and protect themselves within it.

4 Conclusion

The widespread use of the internet among young people has been accompanied by a growing exposure to cyber risks, including online bullying, unsafe social networks, digital scams, and violations of personal privacy [1],[4]. Previous research has shown that awareness of online dangers does not always align with actual behavior. Many young users report having basic knowledge about online privacy, yet they continue to share personal information in uncontrolled ways [4]. This disconnect highlights the need to measure not only knowledge, but also the attitudes and concrete practices of young people regarding digital safety.

In Albania, research on online safety among youth remains limited. Partial reports from international organizations such as UNICEF and Save the Children have emphasized the presence of digital bullying and the lack of systematic education on the safe use of technology [4], [5]. However, standardized quantitative studies analyzing the actual behaviors and perceptions of Albanian youth regarding data protection and digital interaction are still lacking.

From a theoretical perspective, this area of study is supported by models such as the Theory of Planned Behavior [6] and the Protection Motivation Theory [7], which explain that safety-related behaviors are influenced by perceived risk, self-efficacy, and potential benefits. These models have been widely applied to understand decision-making in information security contexts [8], [15].

More recent studies on youth across the Balkan region reveal an alarming trend: a significant overlap between social media use and high exposure to inappropriate content, interactions with strangers, and uncontrolled sharing of personal information [9]. These findings reinforce the need for localized research that assesses approaches to online safety within the social and cultural context of countries like Albania, where digital education is still in development.

This study, based on a structured and online-distributed survey, aims to fill this gap by offering a detailed overview of:

• the online behaviors of Albanian youth,

•their perceptions of digital risks and personal privacy,

• and the relationship between knowledge, attitudes, and actual behaviors in response to online threats.

It contributes to the existing literature by providing new data that can support the design of educational policies, raise community awareness, and inform the development of customized training programs at both the school and national levels.

Ultimately, a lack of cybersecurity awareness and education among youth poses a significant risk not only at the individual level but also to society at large. An uninformed young population can become an unintentional enabler of cyber threats, acting as an open gateway for malicious attacks. If not addressed, this vulnerability may evolve into a systemic weakness, compromising national security, privacy, and public trust. Cybersecurity education must therefore be prioritized as a foundational element of digital citizenship and societal resilience.

Acknowledgement:

We would like to express our gratitude to the Mediterranean University of Albania for supporting this paper, LAIA project, Cost Action CA22104, (BEiNG – WISE).

References:

[1] Livingstone, S., and Helsper, E.J., *Gradations in digital inclusion: Children, young*

people and the digital divide, New Media & Society, vol. 9, no. 4, pp. 671–696, 2007.
[2] Boyd, D., *It's Complicated: The Social Lives of Networked Teens*, Yale University Press, 2014.
[3] Youn, S., *Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents*, Journal of Consumer Affairs, vol. 43, no. 3, pp. 389–418, 2009.
[4] UNICEF Albania, *Child online protection in Albania: National report*, UNICEF, 2021. [Online]. Available: https://www.unicef.org/albania
[5] Save the Children Albania, *Digital Risks and Child Safety Online*, Tirana, 2022.
[6] Ajzen, I., *The theory of planned behavior*, Organizational Behavior and Human Decision Processes, vol. 50, no. 2, pp. 179–211, 1991.
[7] Rogers, R.W., *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*, In: Cacioppo, J.T., Petty, R.E. (Eds.), *Social Psychophysiology*, Guilford Press, pp. 153–176, 1983.
[8] Anderson, C.L., and Agarwal, R., *Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions*, MIS Quarterly, vol. 34, no. 3, pp. 613–643, 2010.
[9] Krasniqi, A., Sadiku, A., and Meta, G., *Social media use among Balkan youth and exposure to online risks*, Journal of Balkan Studies, vol. 5, no. 2, pp. 88–105, 2021.
[10] Marku, D., and Leka, A., *Digital literacy and online safety among Albanian high school students*, Albanian Journal of Education and Technology, vol. 3, no. 1, pp. 45–58, 2020.
[11] Marwick, A.E., and Boyd, D., *Networked privacy: How teenagers negotiate context in social media*, New Media & Society, vol. 16, no. 7, pp. 1051–1067, 2014.
[12] Nadiia Karlova, Iryna Kotienieva, Juliia Kotienieva, Olena Sievastianova, Iryna Pavlenko, *"The Influence of Interactive Web Platforms on the Development of Future Specialists' Communication Competences,"* WSEAS Transactions on Information Science and Applications, vol. 21, pp. 291-302, 2024, DOI:10.37394/23209.2024.21.28
[13] Abdulatif Alabdulatif, *"The Role of Cybersecurity in Confronting Intellectual Security Threats,"* WSEAS Transactions on Information Science and Applications, vol. 20, pp. 189-196, 2023, DOI:10.37394/23209.2023.20.22
[14] Hyka, D., & Kodra, F. (2025*). "Cybersecurity in Albanian Accounting: Enhancing Data Integrity and Risk Management."* Smart Cities and Regional Development (SCRD) Preprints, 2(1).
[15] Qordia, G., & Dolantina, H. Y. K. A. (2024). *The benefits of using IPA in relation to RPA for the cryptocurrency sector, in making decisions on their sale and purchase in the stock market.* Smart Cities and Regional Development (SCRD) Journal, 8(2), 31-38.