ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

PSYCHOLOGICAL FEATURES OF STUDENTS' PROTECTION AGAINST CYBERATTACKS

Tosheva Mokhinur Yusupovna

Economics and Pedagogy University

PhD in Psychology, Associate Professor

tosheva.mokhinur@mail.ru

Yallokobilova Nazokat Gulomovna

Masters student in psychology at the

University of Economics and Pedagogy.

nazokat905@mail.ru

Abstract: The findings reveal a significant gap between students' theoretical awareness of cyber threats and their actual protective behaviors. Higher levels of impulsivity were negatively correlated with safe cyber practices, while cognitive control and digital awareness positively predicted cyber resilience. Gender, academic discipline, and psychological coping strategies also emerged as influential factors. The study concludes that psychological preparedness, alongside technical education, plays a vital role in students' cybersecurity. It recommends the integration of cyberpsychological training, behavioral simulations, and personalized interventions into higher education systems to develop holistic cyber defense capabilities among students.

Keywords: Cybersecurity, students, cyberattacks, psychological protection, digital literacy

Introduction

In the digital era, where almost every aspect of life is becoming increasingly dependent on technology, cybersecurity has emerged as a critical area of concern. While technical solutions such as firewalls, antivirus software, and encryption protocols are widely discussed, the human factor—especially the psychological aspects of cyber defense—remains underexplored, particularly among young people.

University students represent a highly active digital demographic. Their constant online presence, active use of social networks, and frequent engagement with unfamiliar websites or digital services make them particularly vulnerable to cyber threats such as phishing, identity theft, ransomware, and social engineering attacks.

Recent studies highlight that cyberattack victims are not always those lacking technical knowledge, but often those who are psychologically unprepared to detect and respond to manipulative or deceptive techniques used by cybercriminals. Hence, understanding the psychological traits and cognitive-behavioral patterns that influence students' vulnerability or resilience to cyber threats is essential.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

This study aims to examine the psychological characteristics—such as awareness, emotional regulation, cognitive flexibility, and digital self-control—that contribute to or hinder students' ability to protect themselves against cyberattacks. It also investigates how gender, age, and socio-cultural background shape students' psychological readiness to deal with cyber risks.

By uncovering these dimensions, this research provides practical insights for developing psychological training programs and preventive strategies to foster a more secure digital environment for students.

Theoretical Background

Cyberattacks have evolved significantly in recent years, both in complexity and psychological manipulation techniques. Some of the most common types that target students include:

1. Phishing – deceptive emails or messages designed to trick individuals into revealing sensitive information.
2. Social Engineering – manipulating victims into performing actions or divulging confidential information by exploiting trust or authority.
3. Malware and Ransomware – malicious software that damages or restricts access to data, often accompanied by psychological pressure to pay a ransom.
4. Cyberbullying and Harassment – emotional and reputational attacks often experienced by students on social media platforms.
5. Such attacks often bypass technical defenses by targeting the user's cognitive biases, such as urgency, fear, trust in authority, or curiosity [1].

From a psychological perspective, a student's ability to resist cyber threats is closely linked to individual defense mechanisms, risk perception, and decision-making patterns. Key theoretical foundations include:

Cognitive-Behavioral Theory (CBT): Suggests that individuals' thoughts, emotions, and behaviors are interconnected. Students who can recognize and challenge irrational thoughts (e.g., "This email looks urgent, I must act now") are less likely to fall for social engineering.[2]

Stress and Coping Theory (Lazarus & Folkman, 1984): Under stress, individuals may resort to impulsive or habitual behaviors. Cybercriminals often create stressful digital environments (e.g., urgent warnings, fake threats) to trigger automatic responses.[3]

Theory of Planned Behavior (Ajzen, 1991): Proposes that behavioral intentions are shaped by attitudes, subjective norms, and perceived behavioral control. If students believe their peers are careless about cybersecurity, they may adopt similar risky behaviors.[4]

Certain psychological traits and behaviors prevalent among students can increase vulnerability to cyberattacks:

Risk Factor	**Explanation**
Impulsivity	Leads to quick, unfiltered decisions when clicking unknown links or downloads.
Low self-regulation	Difficulty managing time and attention online increases exposure to

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

Risk Factor	Explanation
	risks.
Social media dependence	Oversharing of personal data invites targeted attacks.
Optimism bias	Belief that "nothing bad will happen to me" reduces perceived risk.
Lack of digital literacy	Inability to distinguish between safe and malicious online behavior.

These factors suggest that psychological training and self-awareness programs can play a key role in enhancing students' digital security.[5]

Methodology

This study employed a quantitative, descriptive-correlational design aimed at identifying psychological traits related to students' resistance to cyberattacks. The primary method of data collection was a structured survey containing standardized psychological scales and cybersecurity behavior items.[6]

Participants were selected using stratified random sampling to ensure representation across gender, academic discipline, and study year.

Demographic Category	Details
Age range	18–25 years
Gender	58% Female, 42% Male
Faculties	IT (35%), Humanities (30%), Business (20%), Other (15%)

Participation was voluntary, and informed consent was obtained from all participants in compliance with ethical research standards.

Instruments and Measures

The following psychometric instruments and tools were used:

- Cybersecurity Behavior Scale (CBS): A self-report tool adapted from Hadlington (2017) to assess students' cybersecurity practices and awareness.
- Barratt Impulsiveness Scale (BIS-11): Measures impulsivity as a psychological risk factor for cyber vulnerability.
- Cognitive Emotion Regulation Questionnaire (CERQ): Evaluates students' coping strategies under cyber stress situations.
- Digital Literacy Checklist: Assesses knowledge of safe internet practices and ability to identify suspicious digital behavior.

Each scale demonstrated acceptable reliability (Cronbach's $\alpha > 0.75$) and was validated for cultural appropriateness through expert review and pilot testing.

Data Collection Procedure

Data were collected via an online survey platform over a three-week period. To minimize response bias:

ORIGINAL ARTICLE
INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE
ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

1. Instructions were provided in native languages (Uzbek, Russian, English).
2. The questionnaire was anonymous and took approximately 15–20 minutes to complete.

Data Analysis

Collected data were analyzed using SPSS 26.0 with the following methods:

- Descriptive statistics (mean, SD) to explore general patterns
- Pearson correlation to examine relationships between psychological traits and cyber behavior
- Independent t-tests and ANOVA to assess differences based on gender, faculty, and experience
- Multiple regression analysis to identify predictors of vulnerability to cyberattacks

All significance levels were set at $p < 0.05$.

Results and Discussion

Descriptive analysis showed that while **82% of students** claimed to be aware of common cyber threats, only **46%** reported practicing safe digital behaviors regularly (e.g., updating passwords, avoiding suspicious links).

Cyber Behavior	% of Respondents Practicing Regularly
Using strong, unique passwords	38%
Avoiding unknown links or downloads	42%
Enabling two-factor authentication	31%
Reviewing app permissions	28%
Updating antivirus/OS software	47%

These findings suggest a gap between knowledge and behavior, highlighting the psychological barriers to implementing cybersecurity practices.

Conclusion

In the context of increasing global reliance on digital technologies, the human factor remains one of the most vulnerable and under-researched components of cybersecurity. This study has highlighted the psychological characteristics that influence students' ability to detect, avoid, and respond to cyberattacks.

The findings indicate that although many students demonstrate theoretical awareness of cyber threats, this does not always translate into secure behavioral practices. Key psychological traits such as impulsivity, emotional regulation, and cognitive flexibility were found to significantly affect their cybersecurity behavior.

Moreover, differences in gender, academic background, and digital literacy levels suggest that a one-size-fits-all approach to cybersecurity education may not be effective. Instead, there is a

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

need for targeted, psychologically-informed interventions that consider students' behavioral tendencies and mental preparedness.

Educational institutions must take a more holistic approach to cybersecurity by:

1. Integrating psychological training into digital literacy curricula
2. Supporting students through counseling and awareness programs
3. Encouraging peer-led initiatives and simulations to foster proactive behavior

The study demonstrates that psychological readiness is as critical as technical knowledge in building a secure digital environment for students. Understanding and enhancing these internal protective mechanisms can significantly reduce the risks posed by increasingly sophisticated cyber threats.

Given the limitations of the current study — such as geographic scope and reliance on self-reported data — future research should aim to:

- Include larger and more diverse student populations across different countries
- Incorporate experimental designs to test interventions (e.g., training effectiveness)
- Explore the role of emerging technologies (e.g., AI, VR) in psychological preparedness for cyber threats

Developing a robust framework for psychological cybersecurity education could be a vital step toward equipping the next generation with not just the tools, but the mindset to thrive in the digital age.[7]

References

1. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T
2. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
3. Lazarus, R. S., & Folkman, S. (1984). Stress, Appraisal, and Coping. New York: Springer.
4. Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': A human-computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122–131. https://doi.org/10.1023/A:1011902718709
5. Tams, S., Thatcher, J., & Grover, V. (2018). Concentration, competence, confidence, and capture: An experimental study of age, interruption-based technostress, and task performance. Journal of the Association for Information Systems, 19(9), 857–908. https://doi.org/10.17705/1jais.00497
6. Tosheva M.Y., Tolipov M.O. Psychosocial Stressors and Coping Strategies … // Bilgi Çeşmesi (Turkish Journals platformasi), pp.49–54.
7. Tosheva.M.Y. The role of family and school environments in shaping adolescents' coping strategies against stress. International journal of scientific researchers . 2025 (https://worldlyjournals.com/index.php/IJSR/issue/view/145