CYBERSECURITY AMONG USERS: PERCEPTIONS, KNOWLEDGE, AND REALITIES

UDC: [004.056+004.8]:[658.89+366.14]
DOI: https://doi.org/10.53486/tids2025.11

VERONICA HÎNCU
Academy of Economic Studies of Moldova
soltanici.veronica@ase.md
ORCID ID: 0009-0002-9291-088X

Abstract. In an increasingly digital world, cybersecurity has become a fundamental concern for both individuals and organizations. This paper explores users' perceptions, knowledge, and real-world behaviors related to digital security, based on the analysis of a questionnaire applied to a sample of 100 participants. The study investigates five thematic areas: awareness of cyber threats, personal and organizational experiences, individual security practices, openness to cybersecurity education, and expert perspectives on emerging solutions such as artificial intelligence.

The results reveal a significant gap between theoretical awareness and actual behavior. While 93% of respondents correctly defined a cyberattack, only a small percentage actively apply good cybersecurity practices – such as updating software, using two-factor authentication, or changing passwords regularly. Furthermore, 37% of participants reported having been affected by cyber incidents, yet only a third of organizations reportedly use vulnerability detection tools on a regular basis. A notable proportion of respondents (58%) expressed willingness to participate in cybersecurity training if it were accessible and easy to understand, and over one-third recognized the value of artificial intelligence in enhancing security capabilities.

This contrast between awareness and action underscores the urgent need for targeted digital education, user responsibility, and organizational investment in automated tools. The findings suggest that cybersecurity culture must be redefined as a shared responsibility, where users, institutions, and policymakers align efforts to foster a safer digital environment. The study contributes to a better understanding of the human factor in cybersecurity and outlines key directions for future training, policy, and technological adoption.

Keywords: Cybersecurity, User Awareness, Digital Behavior, Vulnerability Detection, Cyber Threats, Artificial Intelligence.

JEL Classification: D83, L86, O33.

INTRODUCTION

In recent years, the digitalization of everyday life has led to a growing dependence on technology, making cybersecurity not just a technical issue, but a societal necessity. Individuals, organizations, and governments face increasing risks related to data breaches, phishing attacks, identity theft, and other cyber threats. Consequently, the role of users as both potential targets and active participants in ensuring digital safety has become more relevant than ever.

Several studies (Anderson & Moore, 2007; ENISA, 2022) have emphasized that while users may have a general understanding of cybersecurity, their real-life practices often lag behind. This discrepancy between knowledge and behavior has sparked interest in exploring the human factor in cybersecurity – particularly in relation to awareness, preparedness, and willingness to adopt safe practices.

This paper seeks to address the following research questions:

- How aware are users of current cyber threats and vulnerabilities?

- What are their personal and organizational experiences with cyber incidents?
- What behaviors and security measures do they adopt in daily digital interactions?
- Are users open to cybersecurity education and innovation, such as AI-driven tools?

The theoretical framework is grounded in behavior-based cybersecurity models, which highlight how risk perception influences the adoption of protection strategies. The study is exploratory and descriptive, aiming to fill a gap in understanding the digital habits and attitudes of general users – not IT specialists.

The main objective of this research is to analyze the perceptions, knowledge, and realities of cybersecurity among users, based on the results of a structured questionnaire applied to a sample of 100 respondents. The paper contributes to the growing literature on user-centered cybersecurity by identifying gaps between awareness and practice, and by proposing concrete directions for future education, policy, and technological adaptation.

METHODOLOGY

This study employed a quantitative research approach based on the application of a structured questionnaire. The objective was to assess users' perceptions, knowledge, and behaviors related to cybersecurity, focusing on both individual and organizational contexts.

The questionnaire was distributed online and completed by a total of 100 respondents. The sample included participants from various professional backgrounds and age groups, with no prior requirement for technical expertise in cybersecurity. The anonymity of respondents was ensured to encourage honest and accurate responses.

The questionnaire was divided into five thematic sections:

1. **Awareness of Cyber Threats and Vulnerabilities** – aimed to evaluate the respondents' understanding of common cyber risks and threats such as phishing, data breaches, and financial fraud.
2. **Personal and Organizational Experiences** – explored whether respondents had been personally affected by cyber incidents and the extent to which their organizations implemented protective measures.
3. **Cybersecurity Behaviors and Practices** – investigated individual security habits, such as updating software, password management, and use of multi-factor authentication.
4. **Attitudes and Openness to Learning** – examined perceptions regarding responsibility, data protection awareness, and willingness to participate in educational initiatives.
5. **Expert Perspectives (Optional)** – provided respondents with the opportunity to share opinions on advanced topics such as artificial intelligence, organizational vulnerabilities, and proposed solutions.

The collected data were analyzed using descriptive statistical methods, with results presented as percentages to illustrate key trends and behaviors. No personal identifying information was collected. The approach enabled the identification of discrepancies between awareness and actual practice, as well as gaps in organizational preparedness and individual responsibility.

1. FINDINGS AND DISCUSSION

1.1 Awareness of Cyber Threats and Vulnerabilities

The results indicate that most users possess a theoretical understanding of cybersecurity threats. Specifically, **93% of respondents correctly defined a cyberattack** as an unauthorized attempt to access data or systems. This finding reflects a relatively high level of basic awareness regarding the nature of digital risks.

However, when analyzing practical exposure to threats, a more nuanced picture emerges. Nearly **47% of respondents reported having received at least one suspicious email or message** requesting personal information - indicating that phishing remains a common issue, despite general awareness of its existence.

In terms of perceived risks, respondents ranked **financial fraud** as the most significant threat (48%), followed by **system access disruption** (32%), and **loss of personal data** (14%). This prioritization highlights users' concern with direct, tangible consequences of cyber incidents, particularly those with potential financial impact.

These results suggest that while users may be familiar with cybersecurity terminology and concepts, their perception of threats is shaped primarily by personal relevance and perceived severity. It also reflects a reactive mindset, where awareness exists but is not always translated into preventive behavior.

Furthermore, the emphasis on financial fraud as the top concern points to a need for enhanced education on the broader scope of cybersecurity risks, including social engineering, ransomware, identity theft, and data manipulation – threats that can be equally damaging but may not be immediately visible to non-expert users.

1.2 Personal and Organizational Experience

The survey results reveal that cybersecurity incidents are not merely hypothetical for many users. 37% of respondents reported having been directly affected by cyberattacks, including data loss and unauthorized access to personal or work-related accounts. This figure underscores the tangible impact of digital threats and confirms that cyber incidents are a lived reality for a significant portion of the sample.

On the organizational side, the findings are equally concerning. Only 37% of respondents indicated that their organizations regularly use vulnerability detection tools. This suggests that even in professional environments, proactive measures for identifying and mitigating threats are not consistently implemented. The lack of systemic protection may further expose users to risks, especially in hybrid work environments where personal and professional digital spaces often overlap. Moreover, 70% of respondents identified the lack of financial resources and proper training as the main reasons for their organizations' vulnerability to cyber threats. This reflects a structural issue that extends beyond individual behavior, highlighting gaps in strategic investment and workforce development at the organizational level.

These results suggest a dual-layered challenge: on one hand, users face real consequences due to cyber incidents; on the other, the institutions meant to support and protect them may not be adequately prepared. The findings emphasize the need for targeted investment in both technological infrastructure (e.g., vulnerability scanners, monitoring systems) and human capital (e.g., training, awareness programs).

1.3 Cybersecurity Behaviors and Practices

Despite a relatively high level of awareness regarding cyber threats, the actual behaviors of users indicate a worrying lack of proactive security practices. The data reveal a significant gap between knowledge and action:

- Only 7% of respondents reported updating their applications immediately after a new update becomes available. This low percentage highlights a critical vulnerability, as outdated software is a common entry point for cyberattacks.
- 43% of respondents never use two-factor authentication (2FA), despite its growing availability and importance in securing accounts. This omission leaves accounts more susceptible to unauthorized access, especially in cases of password leaks.
- Password hygiene is also poor: 54% of respondents admitted they never change their passwords, while 35% do not check the source of applications or websites before accessing them. These findings indicate that many users engage in risky digital behaviors, either due to lack of awareness of best practices or underestimation of potential consequences.

The results suggest that users tend to adopt a minimal or even passive approach to digital protection. Security behaviors such as regular updates, password management, and source verification – though simple and effective – are not yet embedded in the daily routines of a majority of users.

This behavioral gap points to the need for simplified and accessible cybersecurity training that focuses on habit-building, not just knowledge transmission. Moreover, the low adoption rate of even basic practices reinforces the idea that usability and perceived convenience often override caution, especially in non-technical user populations.

1.4 Attitudes and Openness to Learning

Beyond behavior, users' attitudes toward cybersecurity and their willingness to engage in learning opportunities are critical indicators for long-term improvement. The survey results show a generally positive inclination toward acquiring cybersecurity knowledge – 58% of respondents stated they would participate in a data protection course if it were easy to understand. This openness represents a valuable opportunity for designing educational initiatives tailored to non-specialist audiences.

However, gaps in awareness of existing tools and responsibilities persist. For example, 52% of respondents reported not knowing what vulnerability detection tools, if any, are used within their organizations. This suggests not only a lack of transparency from organizational leadership but also limited communication between IT departments and regular users. Additionally, 59% of participants consider organizations to be primarily responsible for data protection, which may indicate a tendency to delegate responsibility rather than see cybersecurity as a shared duty.

While users recognize the importance of protecting personal and organizational data, there is still a need to strengthen their sense of agency and personal accountability. Bridging the gap between interest and action will require communication strategies that are clear, relatable, and context-specific. Moreover, the findings suggest that many users are not resistant to cybersecurity education – they simply need it to be accessible, relevant, and embedded in their digital routines. Institutions and policymakers should seize this opportunity to introduce tiered learning platforms, awareness campaigns, and gamified content that foster active engagement.

1.5 Perspectives on Emerging Solutions

As part of the optional section of the questionnaire, respondents were invited to share their views on the use of advanced technologies – particularly artificial intelligence (AI) – and to suggest improvements for cybersecurity practices within organizations. The responses provide valuable insight into users' openness to innovation and their perception of future-oriented solutions.

Notably, 37.6% of respondents believe that AI can contribute "very significantly" to the detection of vulnerabilities in digital systems. This reflects a growing trust in intelligent, automated tools as essential components of modern cybersecurity strategies. AI-powered solutions are increasingly being integrated into intrusion detection systems, threat analysis, and anomaly monitoring, offering scalability and speed that human teams alone cannot match.

However, the feedback also suggests a cautious optimism. While many users see the potential of AI, others expressed concerns about its complexity, cost, and implementation transparency. This highlights the importance of combining AI deployment with user education and clear communication, ensuring that such technologies are not perceived as "black box" solutions but as accessible tools that enhance – not replace – human decision-making.

Respondents also offered practical suggestions for improving cybersecurity, such as:

- Developing more interactive and personalized training programs.
- Increasing visibility of security protocols within organizations.
- Encouraging regular internal audits and simulations of attack scenarios.
- Establishing dedicated communication channels between IT departments and general staff.

These perspectives demonstrate that users are not passive actors - they are willing to engage and contribute, provided they are equipped with the right tools, knowledge, and support.

CONCLUSIONS AND RECOMMENDATIONS

This study set out to explore how users perceive cybersecurity, what they know, and how they behave in practice. The results reveal a clear disparity between theoretical understanding and real-world actions. While most respondents were able to identify key threats such as cyberattacks or financial fraud, their day-to-day security habits remain inconsistent and, in many cases, insufficient.

A significant portion of users (37%) have experienced cyber incidents firsthand, yet fundamental security practices such as software updates, two-factor authentication, and password management are not widely adopted. Organizational responsibility is acknowledged, but often not matched by transparent communication or adequate resource allocation. Despite these shortcomings, users show promising openness to learning, and many express trust in the potential of artificial intelligence to improve cybersecurity.

Based on the findings, several key recommendations emerge:

1. **Implement continuous digital education programs** tailored to different knowledge levels, using accessible language and interactive formats.
2. **Promote shared responsibility models** where users, organizations, and policymakers all play active roles in maintaining digital security.
3. **Encourage the adoption of good security habits** by integrating them into routine digital behaviors through gamification, nudges, or policy requirements.
4. **Strengthen organizational infrastructure** by investing in vulnerability detection tools, regular security audits, and transparent communication practices.

5. **Leverage AI responsibly**, ensuring that its implementation is accompanied by adequate user training and ethical oversight.

In conclusion, transforming cybersecurity culture requires more than tools and policies – it demands behavioral change, continuous education, and collaboration. The human factor remains both the weakest link and the greatest potential in digital security.

REFERENCES

1. Anderson, R. and Moore, T., 2007. The economics of information security. *Science*, 314(5799), pp.610–613.
2. ENISA, 2022. *Cybersecurity Culture Guidelines: Behavioural Aspects in Cybersecurity*. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity [Accessed 1 Jun. 2025].
3. Liang, H. and Xue, Y., 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), pp.394–413.