Journal of Engineering Science *Vol. XXXII, no. 3 (2025), pp. 75 - 90*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

https://doi.org/10.52326/jes.utm.2025.32(3).07
UDC 004.056.5:37.018.4

EVALUATION OF CYBERSECURITY TRAINING PERCEPTIONS, ADOPTED PRACTICES AND STRATEGIC DIRECTIONS FOR CAPACITY BUILDING

Ludmila Peca*, ORCID: 0000-0002-4394-2933,
Svetlana Cojocaru, ORCID: 0000-0002-1187-4294,
Marius Dumitraşcu, ORCID: 0009-0006-3547-4558,
Dinu Ţurcanu, ORCID: 0000-0001-5540-4246

Technical University of Moldova and National Institute of Innovations in Cybersecurity CYBERCOR, 168, Stefan cel Mare Blvd., Chisinau, Republic of Moldova
* Corresponding author: Ludmila Peca, *ludmila.peca@isa.utm.md*

Received: .08. 19. 2025
Accepted: 09. 23. 2025

Abstract. This paper presents the results of a study conducted by the National Institute of Innovations in Cybersecurity CYBERCOR on the impact of specialized cybersecurity training on behaviors related to the protection of personal and professional data. The survey was administered immediately after the completion of the training sessions to a sample of 842 participants from public, private, and academic sectors, aiming to assess the level of awareness and adoption of digital security measures. Data analysis revealed significant increases in the use of security tools and practices, such as performing regular backups, encrypting data, and applying advanced protection programs. The results also highlight differences between participant categories, suggesting that training level and access to resources influence security behaviors. The study confirms the effectiveness of practical, context-driven training but also indicates the need for sustained organizational policies, continuous awareness campaigns, and the integration of user-friendly security solutions. These findings contribute to the development of national strategies for strengthening cybersecurity resilience through education and training.

Keywords: *cybersecurity, training, data protection, encryption, awareness.*

Rezumat. Acest studiu prezintă rezultatele unei cercetări realizate de Institutul Național de Inovații în Securitatea Cibernetică CYBERCOR, privind impactul instruirilor specializate în domeniul securității cibernetice asupra comportamentelor de protecție a datelor personale și profesionale. Chestionarul a fost aplicat imediat după finalizarea sesiunilor de instruire unui eșantion de 842 de participanți din sectoarele public, privat și academic, cu scopul de a evalua nivelul de conștientizare și adoptare a măsurilor de securitate digitală. Analiza datelor a evidențiat creșteri semnificative în utilizarea instrumentelor și practicilor de securitate, precum realizarea copiilor de siguranță regulate, criptarea datelor și aplicarea programelor avansate de protecție. Rezultatele subliniază, de asemenea, diferențe între categoriile de

participanți, sugerând că nivelul de pregătire și accesul la resurse influențează comportamentele de securitate. Studiul confirmă eficiența instruirilor practice, adaptate contextului, dar indică și necesitatea unor politici organizaționale sustenabile, campanii continue de conștientizare și integrarea unor soluții de securitate ușor de utilizat. Concluziile contribuie la dezvoltarea strategiilor naționale pentru consolidarea rezilienței cibernetice prin educație și formare.

Cuvinte-cheie: s*ecuritate cibernetică; instruire; protecția datelor; criptare; conștientizare*.

1. Introduction

In the context of accelerated digital transformation, cybersecurity constitutes a fundamental pillar of national resilience. The broadening of access to information technologies, combined with an increasing reliance on digital systems across public administration, the economy, and everyday life, has generated an extensive spectrum of risks and vulnerabilities. These risks target not only critical infrastructures but also citizens, public institutions, and the private sector, thereby requiring an integrated and multi-layered approach to digital security.

Within this framework, cybersecurity education is recognized as a strategic priority with cross-sectoral impact. Beyond the domain of IT professionals, all active technology users must acquire competencies in cyber hygiene and incident response. National policy instruments, such as Law No. 48/2023 on cybersecurity and the National Cybersecurity Program 2023–2027, explicitly emphasize the need to develop human capital and foster a pervasive culture of digital security [1,2].

At the organizational level, human-centric strategies are increasingly prioritized as effective measures for reducing cyber risk, complementing the deployment of advanced technical controls [3,4]. In this regard, the National Institute for Innovations in Cybersecurity CYBERCOR plays a pivotal role by conducting structured training sessions focused on awareness, prevention, and incident response. To ensure the effectiveness of these programs, the training content must be tailored to the actual risk profile of the participants, which requires systematic evaluation of their perceptions, needs, and behavioral patterns.

The present study reports the results of a survey administered to participants in CYBERCOR training sessions held during the first quarter of 2025. The research objectives are to:

Determine the extent to which training has produced measurable changes in cybersecurity-related behavior (cyber hygiene practices).

Assess participant perceptions regarding the usefulness, relevance, and overall satisfaction with training content and methodology.

Identify and map emerging training needs, as directly expressed by the participants.

The findings presented herein are derived from applied research aimed at correlating cybersecurity training with both observable behavioral changes and explicitly stated needs. To provide an accurate representation of the training's impact and the specific characteristics of the target audience, the study was designed with a rigorous methodological framework, as detailed in the following sections.

2. Materials and methods

Study Design. The study employed a cross-sectional design integrating both quantitative and qualitative components, based on the administration of an online questionnaire. The primary aim was to evaluate the impact of cybersecurity training programs on participants' digital security behaviors and to identify their actual training needs.

Participants. A total of N = 842 individuals who attended the training sessions organized by the National Institute for Innovations in Cybersecurity CYBERCOR during the first quarter of 2025 responded to the survey. Participation was voluntary and anonymous.

The gender distribution revealed a predominance of female participants (64.6%, n = 544) compared to male participants (35.4%, n = 298), as illustrated in Figure 1.

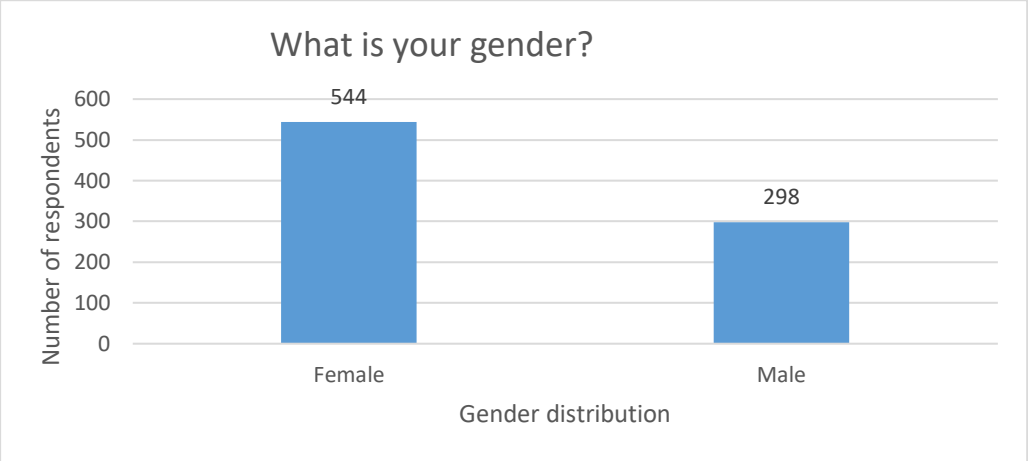

Figure 1. Distribution of respondents by gender (N=842) (question 2 from the survey).
Source: created by the author based on survey results.

Figure 1 highlights an unbalanced gender distribution among participants, with a substantially higher proportion of females (64.6%) compared to males (35.4%). This disparity may influence both the perception profile and the typology of training needs identified within the study.

Regarding the age structure of participants, the survey question *"At the time of completing this questionnaire, you fall into the following age categories"* was used to classify respondents. The analysis of responses shows a predominant concentration within professionally active age groups, which may affect both the level of awareness and the nature of the training needs identified.

Figure 2 presents the distribution of respondents by age categories, providing valuable insights for tailoring training content to the prevailing demographic profile.

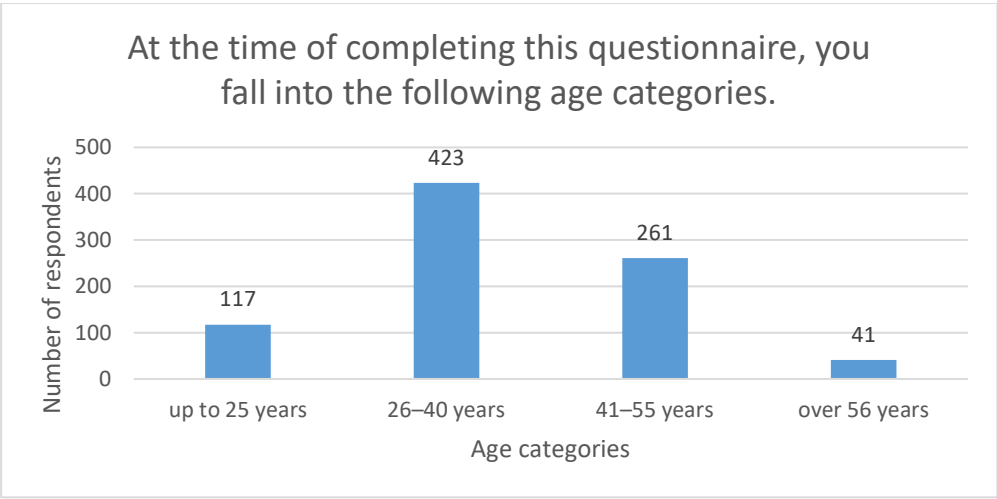

Figure 2. Age distribution of respondents (question 2 from the survey).
Source: created by the author based on the survey results.

The age-group distribution reveals that the 26–40 age segment is the most represented (423 respondents; 50.2%), followed by participants aged 41–55 (261 respondents; 31.0%). This indicates a high level of engagement from individuals in their prime professional years. The under-25 category (117 respondents; 13.9%) and the over-56 category (41 respondents; 4.9%) reflect a steady interest in cybersecurity that extends beyond strictly professional boundaries, confirming the transversal nature of this field.

The distribution of respondents by field of activity (Figure 3) highlights the predominant participation of professionals from the medical sector (30.9%) and the legal sector (20.8%), followed by those from education (13.4%) and from non-governmental or professional organizations (10.8%). Other fields — public service (6.3%), social assistance (5.2%), journalism and communication (3.5%), public administration (1.2%), and finance (0.7%) — accounted for smaller shares, while the "Other" category represented 7.2% of respondents. This structure underscores the multidisciplinary nature of the sample, reflecting the broad applicability of cybersecurity training.

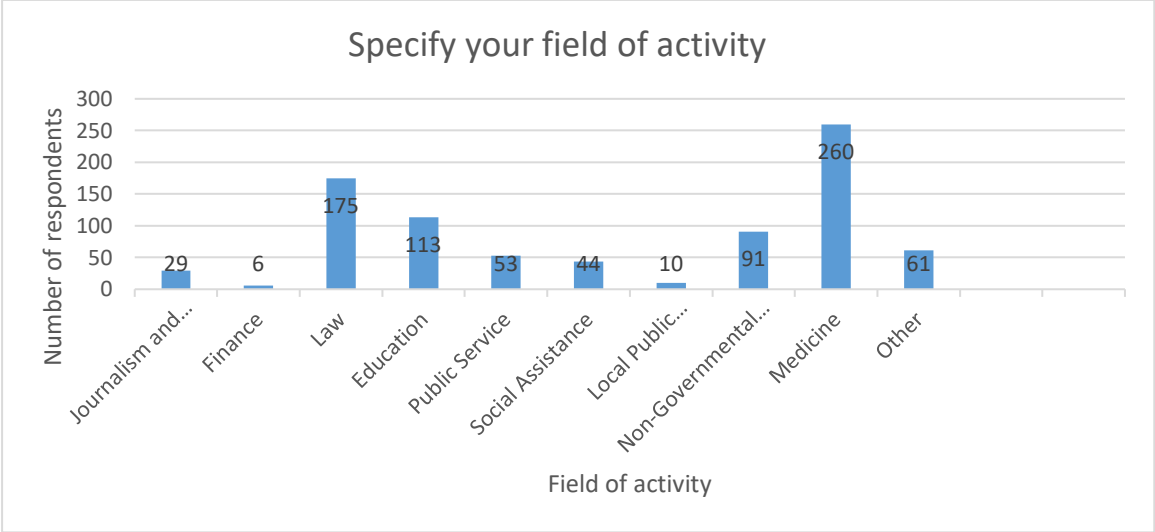

Figure 3. Distribution of respondents by work experience intervals (question 4 of the survey).

Source: created by the author based on the survey results.

Figure 3 illustrates the diversity of participants' fields of activity, with a predominant representation from the medical, legal, and educational sectors. This structure shows that cybersecurity training programs attract both professionals from areas with direct exposure to digital risks and from related sectors, thus increasing the potential for expanding security awareness across multiple professions.

Instrument. The questionnaire used combined closed-ended items (Likert scales, single- and multiple-choice) and open-ended questions, structured into four sections: (1) socio-demographic data and professional profile; (2) perception of the quality and usefulness of the training; (3) current practices and behavioral changes in digital security (passwords, multi-factor authentication – MFA/2FA, software updates, backups, encryption, Google Advanced Protection); (4) training proposals and priorities. The instrument was internally validated by a group of experts in digital education and cybersecurity to ensure the relevance and clarity of the items.

Procedure. The questionnaire was distributed online immediately after the training sessions, with participants being informed and their explicit consent obtained. Data collection was carried out anonymously, without storing personal identifiers.

Indicators and operationalization. Security practices were measured by selecting one of the following options: "already used before training", "adopted after training," "still not using." For multiple-choice items (e.g., 2FA methods – SMS, authentication app, FIDO keys/Passkeys), all selected options were reported as a percentage of the total number of respondents (N=842).

Data analysis. Quantitative data were processed using descriptive statistics (absolute and relative frequencies, with one decimal) and cross-sector comparisons (e.g., MFA/2FA adoption rate in medicine, law, education, NGOs). Responses to open-ended questions were thematically analyzed to identify trends and emerging training directions.

Ethical considerations. The study complied with research ethics principles, ensuring voluntary participation, data confidentiality, and reporting of results exclusively in aggregate form.

Through this methodological framework, the research ensures both scientific rigor and practical relevance of the obtained data, creating the foundation for a detailed analysis of the results. The following section presents the main findings, interpreted in relation to the study objectives and the relevant literature.

3. Results and Discussions

The analysis of the collected responses highlights significant changes in participants' digital security practices, as well as notable differences across sectors of activity. The main findings are presented below, structured according to the study's key indicators and interpreted in relation to the relevant literature and current national policy frameworks.

Before examining the data obtained, it is useful to position them within a theoretical framework based on research into behavior change, which explains how cybersecurity training can lead to the sustainable adoption of secure practices.

Digital behavior change can be explained through the Protection Motivation Theory [5], which emphasizes the role of threat perception and self-efficacy in the adoption of security measures, and the Theory of Planned Behavior [6], according to which the intention to act is determined by attitudes, social norms, and perceived behavioral control. For example, if the work environment supports the use of multi-factor authentication (MFA) and the user feels capable of configuring it, the likelihood of adoption increases substantially [7].

The Transtheoretical Model of Change (TTM) conceptualizes behavioral change as a progression through several stages: precontemplation, contemplation, preparation, action, and maintenance. Training tailored to the stage of each participant (e.g., practical demonstrations for those in the preparation phase) has a higher likelihood of producing lasting change [8].

Empirical research shows that effective training goes beyond information delivery, fostering motivation, self-efficacy, planning, and social support. Interactive methods (simulations, gamified exercises, realistic scenarios) have a substantially greater impact than standard theoretical presentations, with recent meta-analyses confirming a medium-to-large positive effect on end-user behaviors [9,11].

This theoretical framework allows us to interpret the survey data not merely as statistical values but as indicators of respondents' progress along the awareness–adoption continuum of security behaviors.

Guided by these theoretical benchmarks, we analyzed responses to the survey administered to CYBERCOR training participants, with the aim of assessing not only the knowledge acquired but also concrete changes in security behaviors. The following section presents the results for the survey item on perceived training effectiveness (Figure 4), analyzed both in aggregate and across age groups, professional domains, and gender.

Figure 4. Distribution of respondents by work experience intervals (question 4 of the survey).

Source: created by the author based on the survey results.

The distribution of respondents by length of employment provides an important framework for interpreting their perception of training effectiveness. Professional experience can influence both the level of awareness of cybersecurity risks and the openness to adopting new practices.

An essential aspect in evaluating the participants' initial context is the analysis of their prior experience in the cybersecurity field. To this end, the question *"In the past two years, have you received cybersecurity training at your workplace?"* aimed to determine the extent to which respondents had recent training opportunities, either through their employer or on their own initiative.

Figure 5. Previous participation in cybersecurity training (question 5 of the survey).

Source: created by the author based on the survey results.

The data reveal a significant gap in access to formal training, with 64% of respondents reporting no participation in cybersecurity training in the past two years. This finding is concerning, as studies indicate that organizations implementing regular training programs can experience up to 70% fewer security incidents and a 50% lower probability of a breach occurring [12].

Approximately one-quarter of respondents (26.8%) benefited from employer-organized training, while only 9.1% voluntarily attended short-term courses. These results are consistent with the literature, which shows that in the absence of clear institutional policies and a structured training framework, employees' cybersecurity preparedness remains limited [5,9,12]. Organizations such as the National Institute of Standards and Technology (NIST) emphasize that training—unlike simple awareness-raising, is essential for developing real security skills among staff [13].

This underscores the need for periodic programs tailored to the specifics of each activity sector. The study's findings can serve as a strategic foundation for integrating cybersecurity training into annual professional development plans. Official statistics highlight the critical risk posed by human error: over 9 in 10 breaches are caused by carelessness or lack of training, while adequate training can significantly mitigate these risks [14].

Recent literature stresses that the absence of regular training reduces organizational resilience and increases vulnerability to cyberattacks [15]. At the same time, employer-initiated training tends to have a greater impact on the adoption of safe practices than self-initiated courses, due to their integration into the organizational culture and support through internal policies [16].

Another aspect explored was the motivation for participating in cybersecurity training. Question 6 of the survey asked respondents to select the main reason for attending training, choosing a single option from a predefined list.

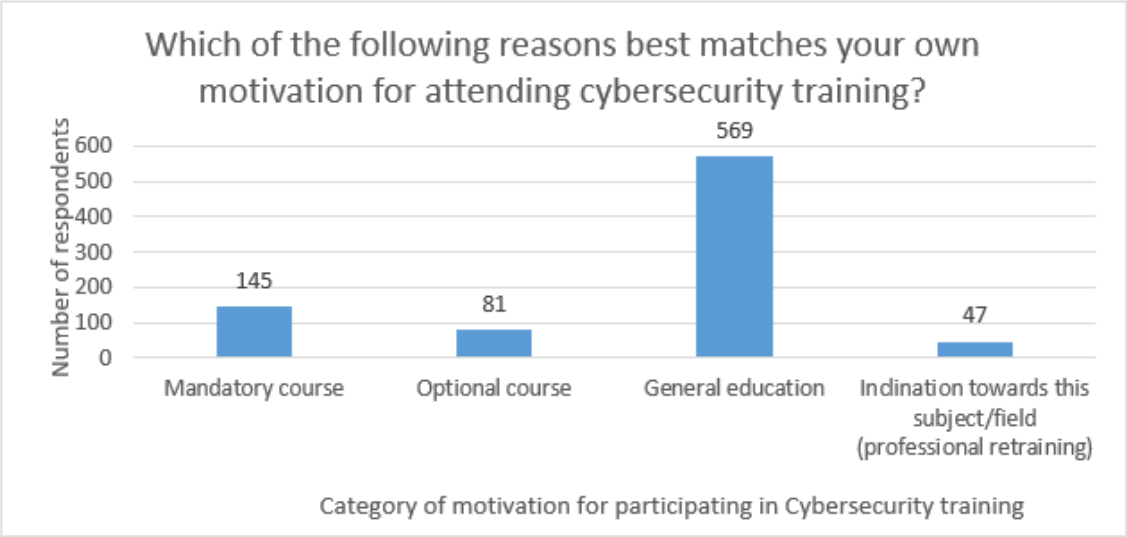

Figure 6. Distribution of responses to the question regarding the main motivation for participating in cybersecurity training (question 6 of the survey).

Source: created by the author based on the survey results.

The results indicate that the most frequent motivation is general education (569 responses), followed by mandatory courses required by the employer (145 responses). Other reasons, such as participation in optional courses (81 responses) or interest in career change/aptitude for this field (47 responses), are significantly less frequently mentioned.

This distribution suggests that, for most participants, training is perceived primarily as an opportunity for personal development and enrichment of general knowledge, rather than as a strict professional requirement. At the same time, the relatively small share of those motivated by career change indicates that current training is not yet a major driver of professional transition, but rather a tool for strengthening general cybersecurity awareness.

These findings are consistent with research on the sustainability of educational processes, which highlights the importance of integrating digital and security competencies into formal education to increase long-term engagement and retention [17]. Consequently, cybersecurity training should be designed not as isolated interventions, but as elements of a continuous strategy for strengthening organizational security culture.

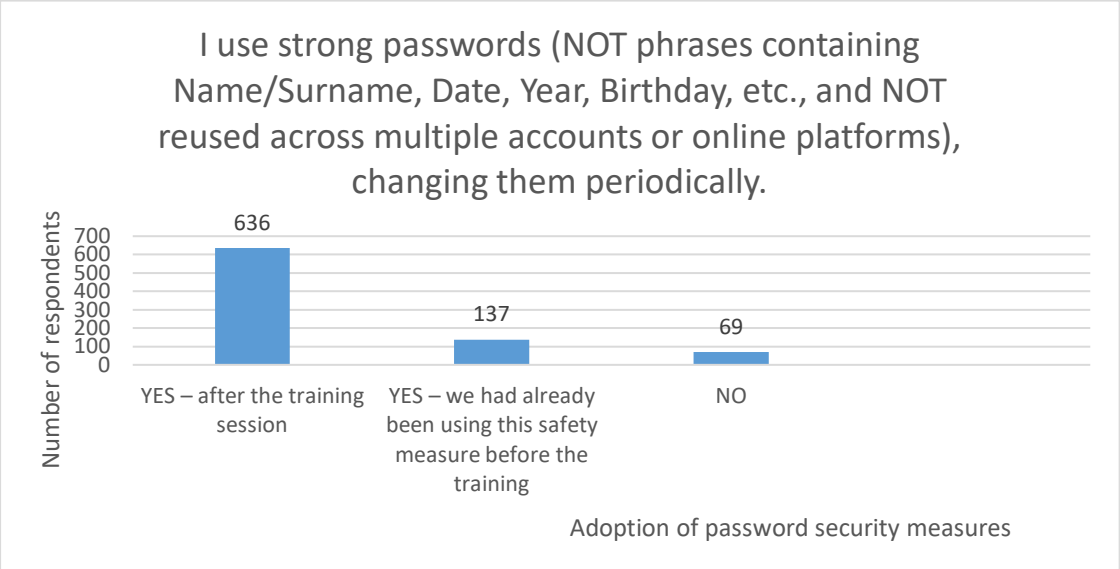

Figure 7. Adoption of cybersecurity measures in relation to training (question 13 of the survey).

Source: created by the author based on the survey results.

Analysis of the responses to the question on the use of strong passwords and their periodic change reveals a significant impact of cybersecurity training on participants' behavior. The data show that 77.6% of respondents (n = 636) began applying this security measure after the training session, suggesting a direct correlation between course participation and the adoption of an essential best practice for account protection. Only 16.7% (n = 137) stated that they had already been applying this practice before the training, confirming the existence of a small segment of users with previously consolidated skills. The percentage of those who still do not use strong passwords remains marginal (5.8%, n = 69), indicating a significant increase in compliance following the training program.

While adopting strong passwords is a first essential step in strengthening account security, the results on the use of multi-factor authentication (MFA) confirm the expansion of security behaviors towards more advanced measures, with a direct impact on reducing the risk of compromise [18]

The data show that 68.7% of participants (*n = 574*) began using multi-factor authentication (MFA) after attending the training, highlighting the role of specialized education in encouraging the adoption of additional protection mechanisms. About 16.4% (*n = 137*) were already applying this measure before the training, confirming the existence of a core group of users previously familiar with good security practices.

However, 15.7% (*n = 131*) still do not use MFA, underscoring the need for intensified awareness campaigns and hands-on training for this category.

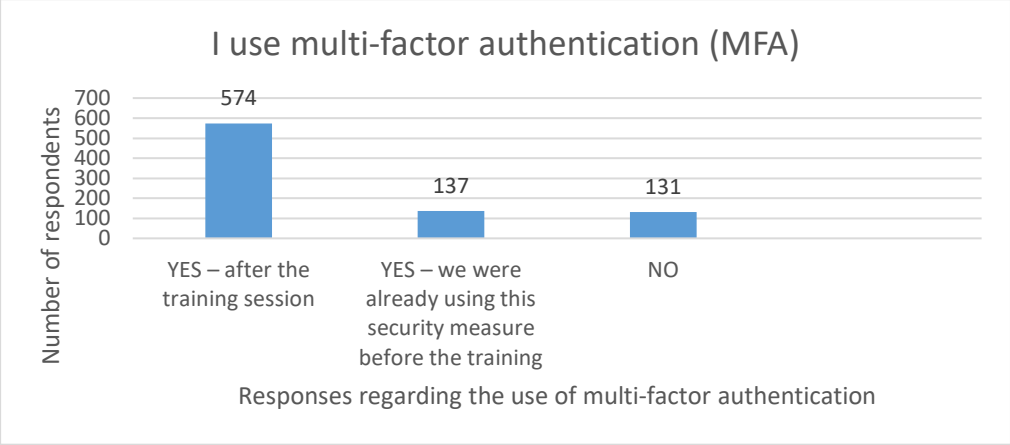

Figure 8. Use of Multi-factor Authentication (MFA) in relation to training (question 14 from the survey).

Source: created by the author based on survey results.

Integrating these results suggests that well-structured training programs not only increase awareness but also drive concrete behavioral changes with direct effects on organizational security. Their recurring implementation can transform these individual practices into sustainable institutional norms, contributing to strengthening cyber resilience.

Continuing the analysis of MFA usage, it is relevant to examine the specific types of 2FA methods adopted by participants to understand their technological preferences and the degree of diversification of applied measures. This detailed perspective allows for evaluating not only adoption levels but also the maturity of implemented solutions from a security standpoint.

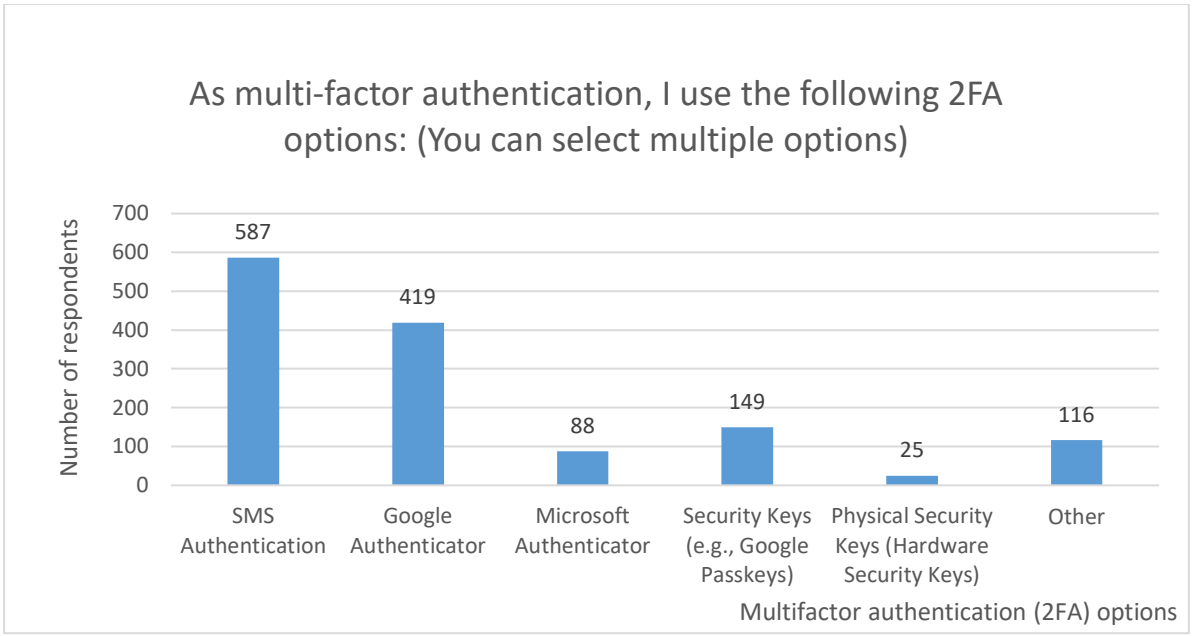

Figure 9. Types of multi-factor authentication (2FA) used by participants after cybersecurity training (question 15 of the survey).

Source: created by the author based on the survey results.

Analysis of the responses regarding the types of multi-factor authentication (2FA) used shows that among participants who apply this security measure, one-time codes generated

by dedicated applications (such as Google Authenticator, Microsoft Authenticator, or Authy) are the predominant option, mentioned by a significant majority. Codes received via SMS also remain a common choice, due to their accessibility and ease of implementation; however, recent research highlights the vulnerabilities of this mechanism compared to solutions based on apps or hardware tokens.

Advanced security methods, such as physical security keys (YubiKey, Titan Security Key) or digital certificates, are used by a smaller percentage of respondents, which may reflect both the higher costs and the need for specialized technical support for implementation. This distribution indicates that while training has contributed to the overall increase in MFA adoption, there is still significant potential for diversifying methods, with a focus on high-security solutions.

Integrating these findings into organizational training strategies could include practical modules dedicated to configuring and using advanced MFA methods, which would increase overall resilience against phishing, SIM swapping, or password compromise attacks.

A detailed analysis of multi-factor authentication (MFA) usage highlights not only the significant increase in adoption rates after training (Figure 9) but also the diversity of methods implemented by participants. While the previous question addressed the presence or absence of MFA as a general practice, the next stage of analysis (Figure 10) explores the specific types of 2FA mechanisms used, providing a more nuanced perspective on post-training security behavior. This approach enables the identification of both technological preferences and potential gaps in the use of more advanced authentication methods.

An integrated analysis of responses shows that training not only stimulates MFA adoption but can also create a favorable context for extending security practices to other critical areas of cybersecurity protection. An essential domain in this respect is the regular updating of software, a fundamental preventive measure to reduce the risk associated with exploitable vulnerabilities. Subsequently, question 16 investigates the extent to which participants keep their operating systems and applications up to date, offering a complementary perspective on the level of accountability and cyber maturity gained after the training.

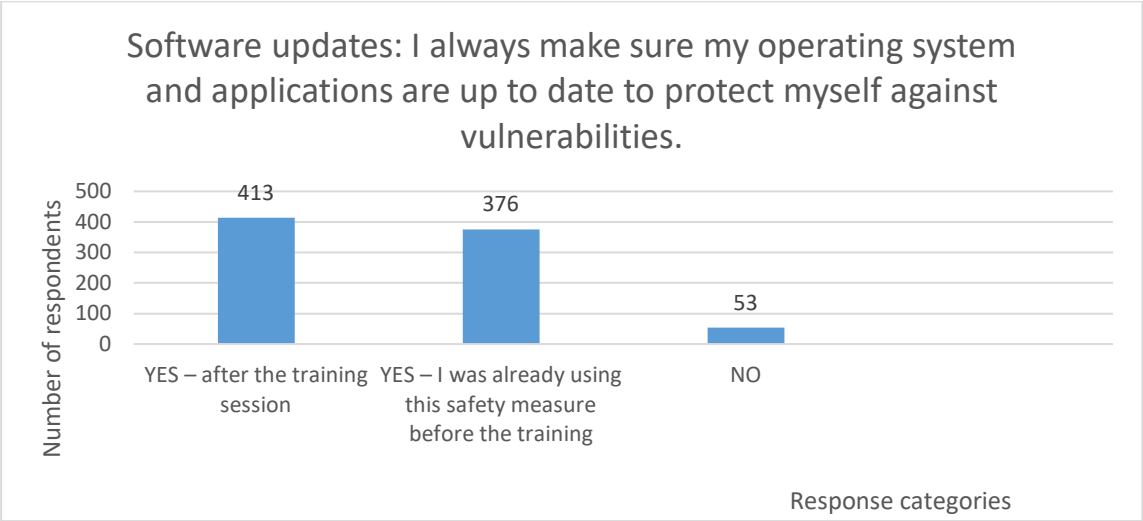

Figure 10. Distribution of responses regarding the frequency of applying software updates (operating system and applications) before and after the training session (survey question 16)**.**

Source: created by the author based on the survey results.

This analysis highlights the importance of maintaining a high level of digital protection, not only through advanced authentication measures but also via proactive policies aimed at reducing software vulnerabilities. In this context, the next evaluated indicator (Figure 11) focuses on the frequency and consistency of updating the operating system and applications. The results show that 413 participants adopted this practice after the training, 376 were already applying it beforehand, and 53 had not implemented it. This distribution provides a clear perspective on the impact of the training and underscores the need to continue integrating modules on software update management into training programs to strengthen protection against vulnerability exploitation.

The results indicate a significant increase in the frequency of applying software updates after the training session, confirming the effectiveness of educational interventions in strengthening proactive security practices. This behavioral shift is essential for reducing exposure to exploits associated with software vulnerabilities, supporting findings from studies that show regular system updates are among the most effective and cost-efficient measures for preventing cybersecurity incidents [19,20].

The analysis of the results in Figure 12 reveals a clear increase in participants' intention to implement regular backup measures after the training session. The majority of respondents (549) stated they would perform periodic backups after training, compared to only 164 who had already been doing so beforehand. However, a significant number (129) still do not apply this measure, indicating a critical area where training efforts must be strengthened.

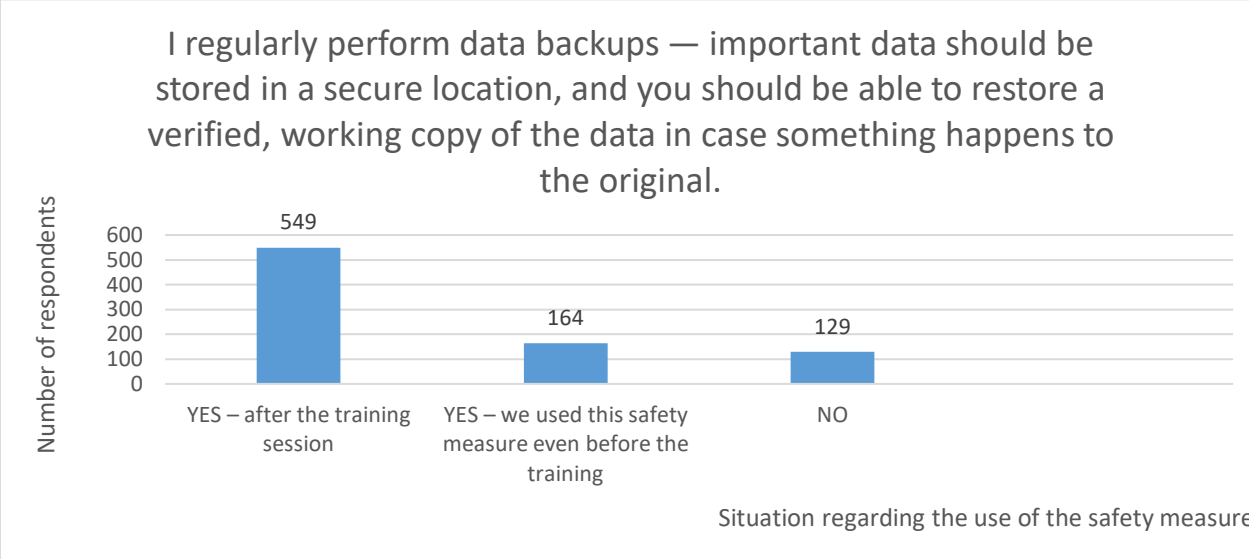

Figure 11. Distribution of participants according to the implementation of periodic data backups before and after the training session (question 17 from the survey).

Source: Author's own compilation based on the survey results.

The results confirm the hypothesis that practical, context-based training can positively influence behaviors related to data security, especially in the area of periodic backups. However, the persistence of a significant proportion of users not engaged in this practice highlights the need for complementary strategies, such as ongoing awareness campaigns, integration of automated backup systems into IT infrastructure, and data recovery simulations [21].

Based on these findings, the analysis extends to another critical element of information protection, data encryption. This practice provides an additional layer of defense against unauthorized access, playing a vital role in preventing sensitive information leaks. The

following section (Figure 13) presents data on the degree of adoption of data encryption by participants, enabling an assessment of cybersecurity maturity from the perspective of applying advanced technical measures.

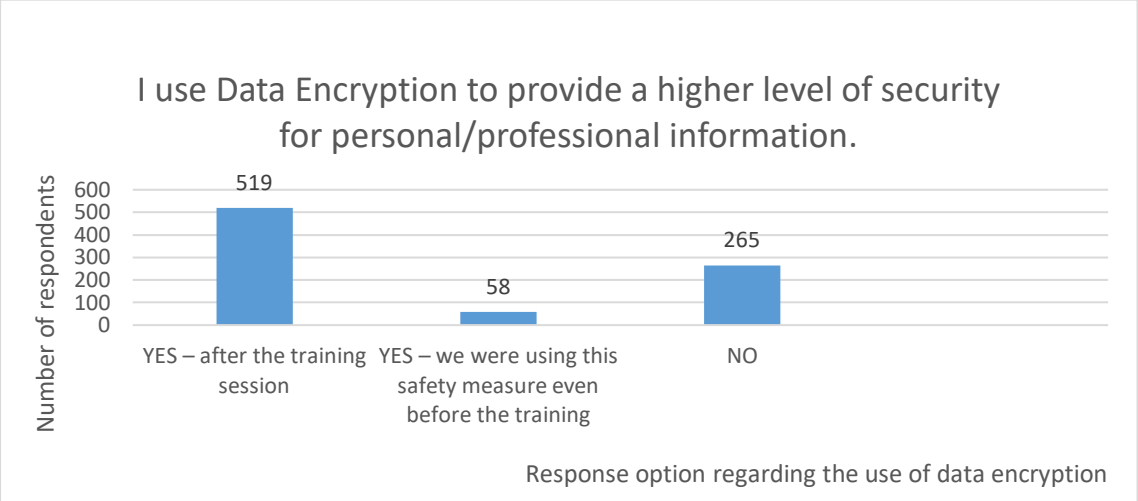

Figure 12. Distribution of responses regarding the use of data encryption for securing personal and professional information (question 18 from the survey).

Source: created by the author based on the survey results.

Analysis of the data presented in Figure 13 highlights the training's impact on increasing the adoption of data encryption. A significant majority of respondents (n = 519, 69.1%) began using data encryption after participating in the training session, underscoring the decisive role of specialized training in promoting this advanced technical protection measure.

At the same time, only 7.7% of participants (n = 58) used this practice before the training, indicating that, in the absence of educational intervention, the adoption rate of this measure would have remained low. However, 35.3% (n = 265) still do not apply encryption, revealing the existence of technical, organizational, or attitudinal barriers preventing its adoption.

The results confirm the hypothesis that practice-oriented training tailored to context can significantly increase the adoption of data encryption, transforming it from a rare practice into a standard for protecting sensitive information [22]. The more than eightfold increase in the number of users applying encryption after training demonstrates the potential of well-structured educational interventions. Nevertheless, the reported non-use rate of over one-third of participants underscores the importance of implementing mandatory organizational policies and facilitating access to user-friendly and efficient software solutions. These findings are consistent with the literature, which indicates that encryption adoption is influenced by both the level of technical competence and the perceived usefulness of encryption in relation to perceived risks [23].

This upward trend in implementing advanced security measures indicates strong potential for adopting other specialized solutions designed to protect high-risk user categories. In this context, a relevant example is the Google Advanced Protection Program / Enhanced Protection Program, designed to provide a higher level of security against targeted attacks and sophisticated threats, especially for individuals handling sensitive data or facing repeated attacks. Analyzing the adoption rate of this program (Figure 15) allows for the evaluation not only of awareness regarding such tools, but also of the practical barrier represented by additional configuration and maintenance requirements, which can affect large-scale adoption.

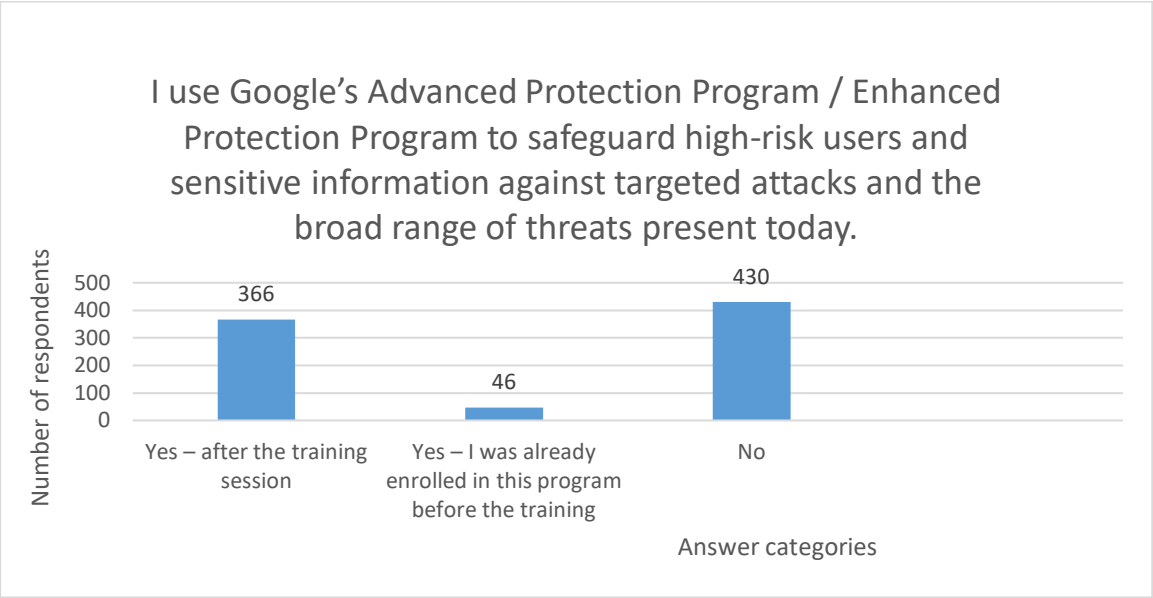

Figure 13. Use of the Google Advanced Protection Program before and after the training session (question 19 from the survey).
Source: created by the author based on the survey results.

The results show that a significant number of respondents (n = 366) began using the Google Advanced Protection program after the training session, compared to those who were already enrolled (n = 46). However, a notable proportion (n = 430) still do not use this advanced security measure.

These data highlight the fact that, although educational interventions have encouraged the adoption of advanced protection solutions for high-risk users, large-scale adoption remains limited. Additional measures are likely needed: clear organizational policies, streamlined enrollment processes, or practical training sessions that explain and facilitate the use of advanced tools.

This observation is supported by recent developments: Google has expanded access to Google Advanced Protection by introducing passkey support, providing more accessible yet robust alternatives to traditional physical security keys [24].

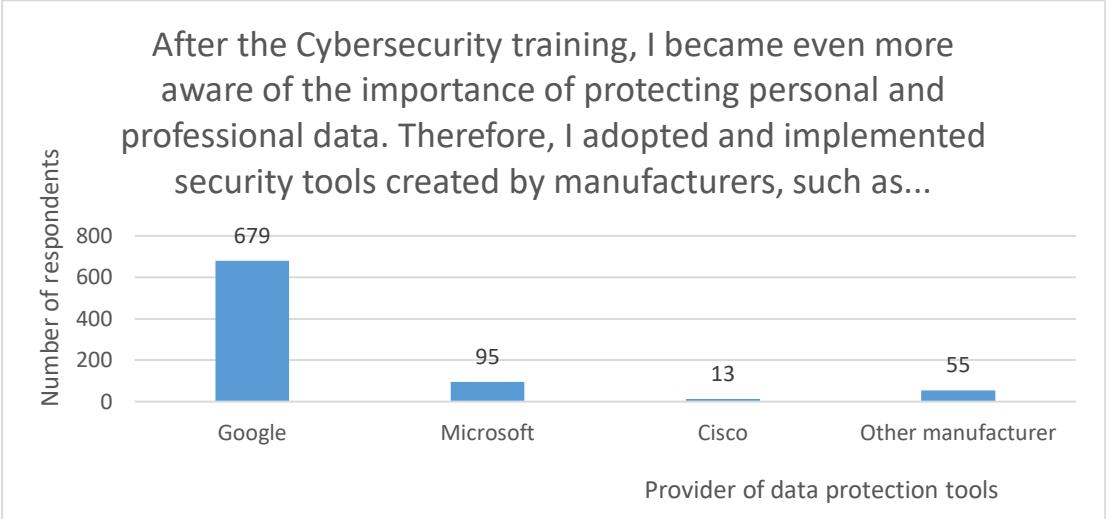

Figure 14. Distribution of participants by adoption of security tools developed by different vendors after cybersecurity training (question 20 of the survey).
Source: created by the author based on the survey results.

The results regarding the level of use of advanced protection programs confirm that targeted training can stimulate the adoption of solutions dedicated to high-risk users. However, the high rate of non-participation suggests the existence of barriers related to awareness, perceived usefulness, and access to resources. In this context, an essential step in strengthening cybersecurity is the adoption of tools and services provided directly by vendors, offering enhanced protection and native integration into the technological ecosystems in use. This aspect is addressed in the following analysis, which explores participants' preferences after training in terms of selecting and implementing such solutions.

The results show a strong concentration of user preference toward Google's solutions, with adoption rates more than seven times higher than those for the next vendor, Microsoft. This distribution can be explained by the familiar interface, direct integration with frequently used services (Gmail, Google Drive), and the reputation of advanced account protection measures for high-risk users.

The low adoption levels for Microsoft, Cisco, and other vendors may indicate either insufficient promotion of these solutions among users or a lower perceived usefulness. Recent studies confirm that perceived accessibility and compatibility with the daily work environment are decisive factors influencing the choice of a particular security ecosystem [25,26].

4. Conclusions and Recommendations

Analysis of the survey results conducted immediately after the cybersecurity training revealed a significant positive impact on participants' awareness level and digital behavior. Following the training activities, they demonstrated a deeper understanding of current cyber threats and an increased ability to adopt measures for protecting both personal and professional data.

The training structure — based on case studies, simulations, and practical exercises, facilitated the transfer of knowledge that could be applied immediately in the professional environment, confirming the relevance of the interactive approach in cybersecurity education. A notable outcome is the increased use of advanced solutions such as multi-factor authentication, data encryption, and security monitoring tools.

The National Institute of Innovations in Cybersecurity CYBERCOR provided the optimal setting for the training, offering advanced-level technical infrastructure and specialized expertise. Through its facilities and the involvement of its team of trainers, CYBERCOR supported the development of critical skills for protecting the cyberspace.

Based on the conclusions drawn from the data analysis and their correlation with the specialized literature, the following action directions are proposed to increase the efficiency of training programs and reduce cyber risks at the organizational level:

1. Institutionalize periodic training programs tailored to the participants' risk profiles.
2. Extend these programs to sectors with critical infrastructure and high exposure to cyber threats.
3. Implement a post-training evaluation mechanism to monitor knowledge retention and adapt the content accordingly.
4. Strengthen partnerships between the public sector, private sector, and academic institutions to promote innovation and the exchange of best practices in the field.

The coordinated and sustained implementation of these measures can significantly contribute to enhancing organizational resilience against cyber threats and to consolidating a long-term security culture.

Acknowledgments: The authors note that these findings informed CYBERCOR's application RFA-2025-001 to the Innovate Moldova Programme.

Conflicts of interest. The authors declare no conflicts of interest.

References

1. Government of the Republic of Moldova. Law No. 48/2023 on Cybersecurity [in Romanian]. Official Gazette of the Republic of Moldova, No. 151–153, 28 April 2023. Available online: https://www.legis.md/cautare/getResults?doc_id=136732&lang=ro (accessed on 2 August 2025)
2. Ministry of Information Technology and Communications of the Republic of Moldova. National Cybersecurity Program 2023–2027, Chișinău, Moldova. Available online: https://old.mtic.gov.md/ro/projects/programul-de-securitate-cibernetica (accessed on 4 August 2025) [in Romanian].
3. Iyer, S.S.; Raji, B. Cybersecurity Culture and Organizational Resilience: A Human-Centered Approach to Digital Risk Management. *American Journal of Industrial and Business Management* 2025, 15, pp. 748–766.
4. Uchendu, B.; Nurse, J. R. C.; Bada, M.; Furnell, S. *Developing a Cyber Security Culture: Current Practices and Future Needs*. Preprint, 2021. Available online: https://arxiv.org/abs/2106.14701 (accessed on 13 August 2025).
5. Rogers, R.W. A Protection Motivation Theory of Fear Appeals and Attitude Change. *J. Psychol*. 1975, 91(1), pp. 93–114.
6. Ajzen, I. The Theory of Planned Behavior. *Organ. Behav. Hum. Decis. Process* 1991, 50(2), pp. 179–211.
7. Ifinedo, P. Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Comput. Secur.* 2012, 31(1), pp. 83–95.
8. Prochaska, J.O.; DiClemente, C.C. Stages and Processes of Self-Change of Smoking: Toward an Integrative Model of Change. *J. Consult. Clin. Psychol.* 1983, 51(3), pp. 390–395.
9. Parsons, K.; Butavicius, M.; Delfabbro, P.; Lillie, M. Predicting Cybersecurity Behaviour: The Role of Protection Motivation, Conscientiousness and Work Engagement. *Front. Psychol.* 2019, 10, 898.
10. Ng, B.-Y.; Kankanhalli, A.; Xu, Y. Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decis. Support Syst.* 2009, 46(4), pp. 815–825.
11. Tam, L.; Glassman, M.; Vandenwauver, M. The Psychology of Password Management: A Tradeoff between Security and Convenience. *Behav. Inf. Technol.* 2010, 29(3), pp. 233–244.
12. Organizations that implemented regular cybersecurity training experienced a 70 % decrease in incidents and 50 % lower probability of breach. Aberdeen Group, 2019. Available online: https://www.aberdeen.com/cybersecurity-training-impact/ (accessed on 12 August 2025)
13. Merritt, M.; Hansche, S.; Ellis, B.; Sanchez-Cherry, K.; Nethery Snyder, J.; Walden, D. Building a Cybersecurity and Privacy Learning Program, 2024. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf (accessed on 12 August 2025).
14. ISACA, Security Awareness Training: A Critical Success Factor for Organizations, 2023. Available online: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/security-awareness-training-a-critical-success-factor-for-organizations (accessed on 12 August 2025).
15. Peca, L.; Țurcanu, D. Reducing Cyber Risk Through a Human–Centred Approach. *Journal of Engineering Science* 2025, 32(1), pp. 18–31.
16. Țurcanu, D.; Peca, L.; Prisacaru, A.; Țurcanu, T. Cyber Security Professional Development within CYBERCOR," *Journal of Engineering Science* 2025, 32(2), pp. 87–98.
17. Peca, L., Dumbraveanu, R., Țurcanu, D. The Sustainability of E-Learning in Higher Education. *Journal of Social Sciences* 2024, 7(3), pp. 111–129.
18. Weinert, A. Your Pa$$word doesn't matter. Microsoft Security Blog. Available online: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984 (accessed on 12 August 2025).
19. Cybersecurity Threat Landscape 2023. European Union Agency for Cybersecurity. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed on 13 August 2025).
20. National Institute of Standards and Technology. Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf (accessed on 4 August 2025).

21. National Institute of Standards and Technology. Guide for Data Backup and Recovery. Special Publication 800-184. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf (accessed on 13 August 2025).
22. Barker, E. Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms (SP 800-175B Rev.1). National Institute of Standards and Technology, 2020. Available online: https://doi.org/10.6028/NIST.SP.800-175Br1 (accessed on 13 August 2025)
23. ENISA. Cryptographic Products and Services Market Analysis, Final v1.0, August 2024. Available online: https://www.enisa.europa.eu/sites/default/files/2024-11/Cryptographic_Products_and_Services_Market_Analysis_Final_Draft_v.9_clean_0.pdf (accessed on 13 August 2025).).
24. Passkeys are now available for high risk users to enroll in the Advanced Protection Program. Google Security Blog, July 10, 2024. Available online: https://blog.google/technology/safety-security/google-passkeys-advanced-protection-program/ (accessed on 9 August 2025).
25. Riasat, I.; Shah, M.; Gonul, M. S. Strengthening Cybersecurity Resilience: An Investigation of Customers' Adoption of Emerging Security Tools in Mobile Banking Apps. Computers 2025, 14(4), 129. Available online: https://doi.org/10.3390/computers14040129. (accessed on 11 August 2025).
26. Peca, L.; Ţurcanu, D. Network security: Practical examples solved to be introduced in network security. Tehnica-UTM, Chisinau, RM, 2023, 243 p.

Citation: Peca, L.; Cojocaru, S.; Dumitraşcu, M.; Ţurcanu, D. Evaluation of cybersecurity training perceptions, adopted practices, and strategic directions for capacity building. *Journal of Engineering Science*. 2025, XXXII (3), pp. 75-90. https://doi.org/10.52326/jes.utm.2025.32(3).07.

Submission of manuscripts: jes@meridian.utm.md