Co-funded by
the European Union

RESEARCH REPORT

MULTINATIONAL RESEARCH REPORT

CARRIED OUT WITHIN THE PROJECT

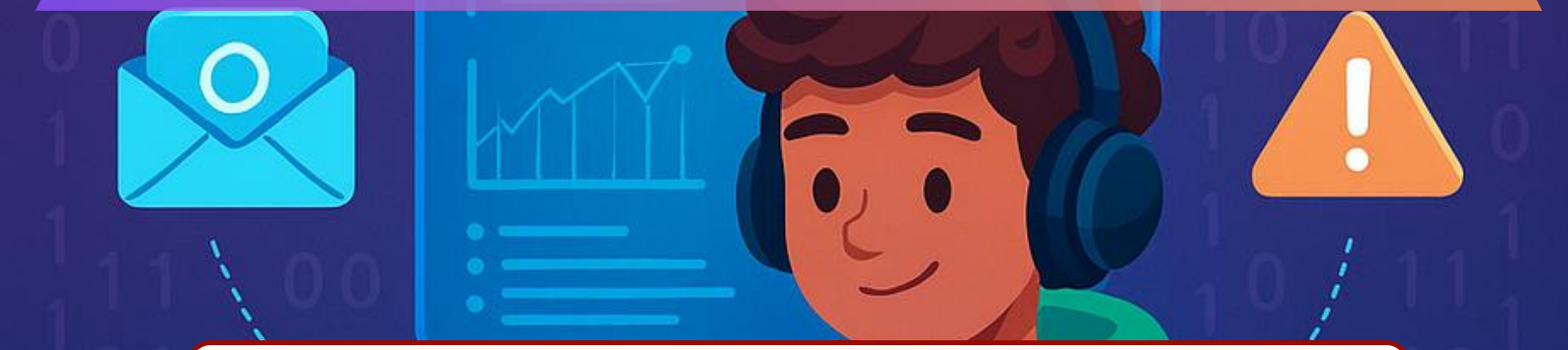
CYBERESCAPE: BUILDING CYBERSECURITY AWARENESS THROUGH GAMIFICATION

CYBERESCAPE

ROMANIA - TÜRKİYE

Co-funded by the European Union

TABLE OF CONTENTS



Co-funded by the European Union

INTRODUCTION

The **CyberEscape** project is a two-year initiative co-funded by the European Union through the Erasmus+ Programme. It aims to strengthen youth resilience against cybersecurity threats by combining research, education, and gamified learning experiences.

Project Objectives

- O1. Increasing by 40% the degree of awareness and competence among 30 youth workers and educators and 300 young people from Romania and Türkiye regarding the topic of critical thinking and managing cybersecurity threats for 24 months.
- O2. Increasing the capacity of defending against cyber threats for youth, (100 directly and 300 indirectly) from Romania and Türkiye during for 24 months.
- O3. Increasing with 25% the organizational capacity of the partners in the consortium by developing the skills of prevention, anticipation, and action in the case of cyber threats and developing a local stakeholder network during the 24 months of project implementation.

Consortium Members:

- Alfa Research Center (ARC) – Applicant organization, based in Oradea, Romania
- ALT357 – Partner organization, based in Bucharest, Romania
- Belen Kaymakamlığı – Partner organization, based in Türkiye

Co-funded by the European Union

WALKTHROUGH

Project Phases:

1. Research
2. Course Development
3. Escape Room Design
4. Testing and Dissemination

This document presents the results of the first phase: the research component. A team of three experts from each consortium member collaboratively designed a questionnaire consisting of 18 items, covering demographics, cybersecurity knowledge, and interest in the topic. The survey received 340 responses—153 from Romania and 187 from Türkiye.

As part of the CyberEscape project, this research phase aimed to gather insights into cybersecurity awareness among young people in Romania and Türkiye. Our goal is to equip youth with the skills needed to navigate the digital world safely and critically. To achieve this, it was essential to first understand who our participants are and the diverse youth contexts they represent.

Through collaborative efforts by the project partners—Belen Kaymakamlığı (Türkiye), ALT357 (Bucharest), and Alfa Research Center (Oradea)—we collected and analyzed data comparing Romanian and Turkish respondents. This allowed us to identify key differences in cybersecurity threats, learning needs, and digital behaviors. The findings reflect a wide range of backgrounds, age groups, and educational stages, highlighting the potential impact of tailored cybersecurity education across varied youth environments.

Co-funded by
the European Union

GROUP PROFILE

The **Romanian participants (N = 153)** represented the more mature side of youth, with the largest share aged 20–24, followed by teenagers (15–19) and smaller groups in their late twenties and thirties. **The Turkish group (N = 187)** was considerably younger overall, with 145 participants (78%) aged 16–19, only 19 participants aged 20–24, 5 aged 25–29, and 18 above 30.

In terms of **gender,** the Romanian group was almost evenly divided between males and females, while the Turkish group showed a clear female majority (112 females, 70 males, and 5 undisclosed). Both groups were predominantly urban-based, but to different degrees: **81%** of Romanian respondents came from cities compared to **76%** in Türkiye, with rural youth representing **19%** in Romania and **24%** in Türkiye.

When it comes to **education,** the Romanian participants showed a broad spectrum: from high school and bachelor's students to those with master's and even postgraduate studies. The Turkish sample, by contrast, was heavily concentrated in secondary education: 83 participants in primary or lower secondary school and 75 in high school. Only 23 participants were pursuing a bachelor's degree and 6 were at master's level.

Occupational status reflected these differences. In Romania, nearly 48% identified as **students**, while a smaller group (6%) was already **employed**. The Turkish respondents, however, were almost entirely **school students**, with very limited representation in **higher education or employment.**

Co-funded by the European Union

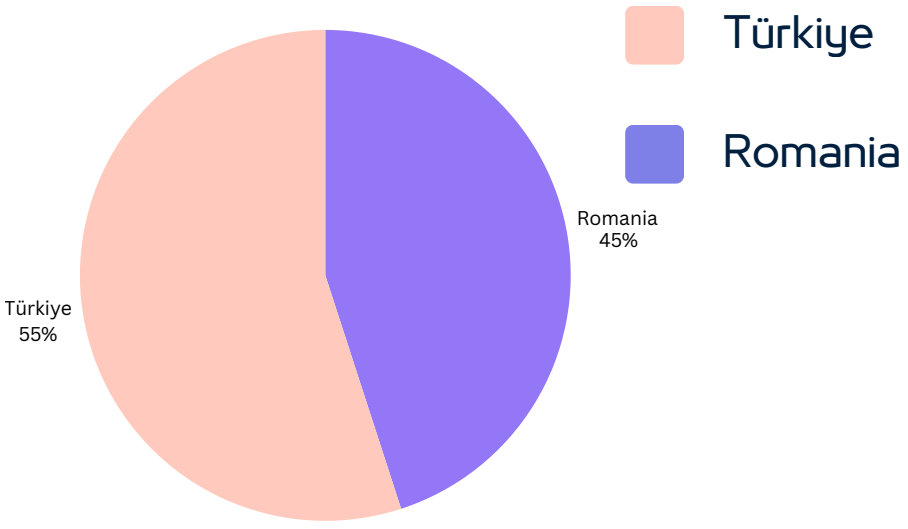
GROUP PROFILE

Countries: Romania and Türkiye

Duration: 1 June 2026 - 21 June 2026

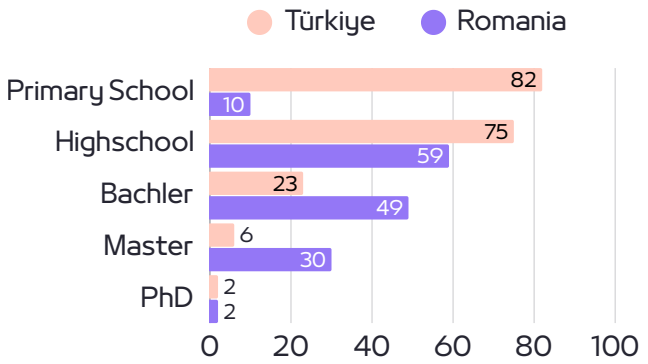
Objective: Awareness regarding cyber security

Responders from Romania and Türkiye



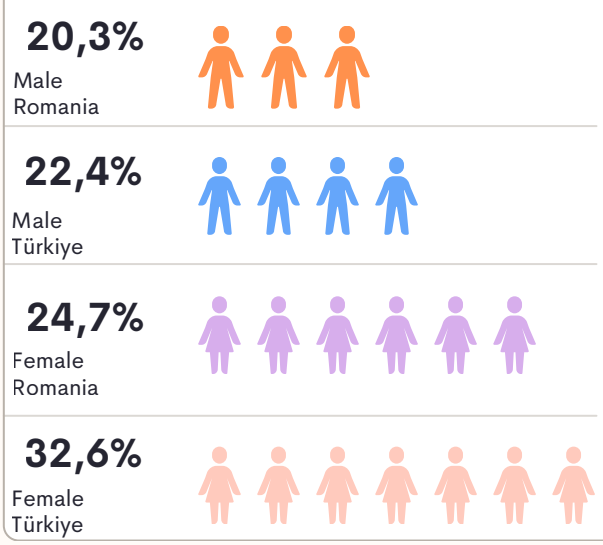
Co-funded by
the European Union

Education

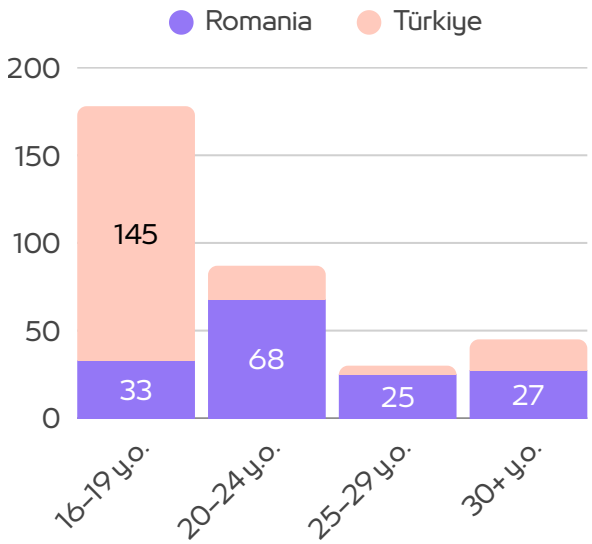


Audience Demographics

Gender



Age Range



Co-funded by the European Union

CYBERSECURITY AWARENESS LEVEL

Understanding how young people perceive their own knowledge of cybersecurity is essential for designing effective training. The results from Romania and Türkiye show both similarities and important differences in awareness levels, which highlight the need for tailored approaches in future interventions.

Romania

When asked about their knowledge of cybersecurity, only 30% of participants felt they truly understood the topic. The majority admitted having only limited knowledge, and around 20% openly stated that they had no real knowledge at all. This indicates that while most young people in Romania have at least heard about cybersecurity, very few feel confident in their understanding. These findings mirror workshop experiences, where participants recognized digital risks but often lacked the tools and skills to handle them independently.

Türkiye

In Türkiye, the results showed somewhat higher levels of awareness. Out of 187 participants, 61 (32%) reported that they had knowledge of cybersecurity, 63 (34%) described their understanding as partial, and 19 (10%) indicated no knowledge. In total, about 75% of Turkish respondents demonstrated either general or partial awareness of cybersecurity issues. However, this self-reported knowledge does not always reflect strong technical understanding or consistent use of safe online behaviors.

Co-funded by
the European Union

COMPARATIVE ANALYSIS

Comparing the two groups reveals a difference in perceived knowledge. In Romania, only 30% felt confident in their understanding of cybersecurity, with a large share reporting limited or no knowledge.

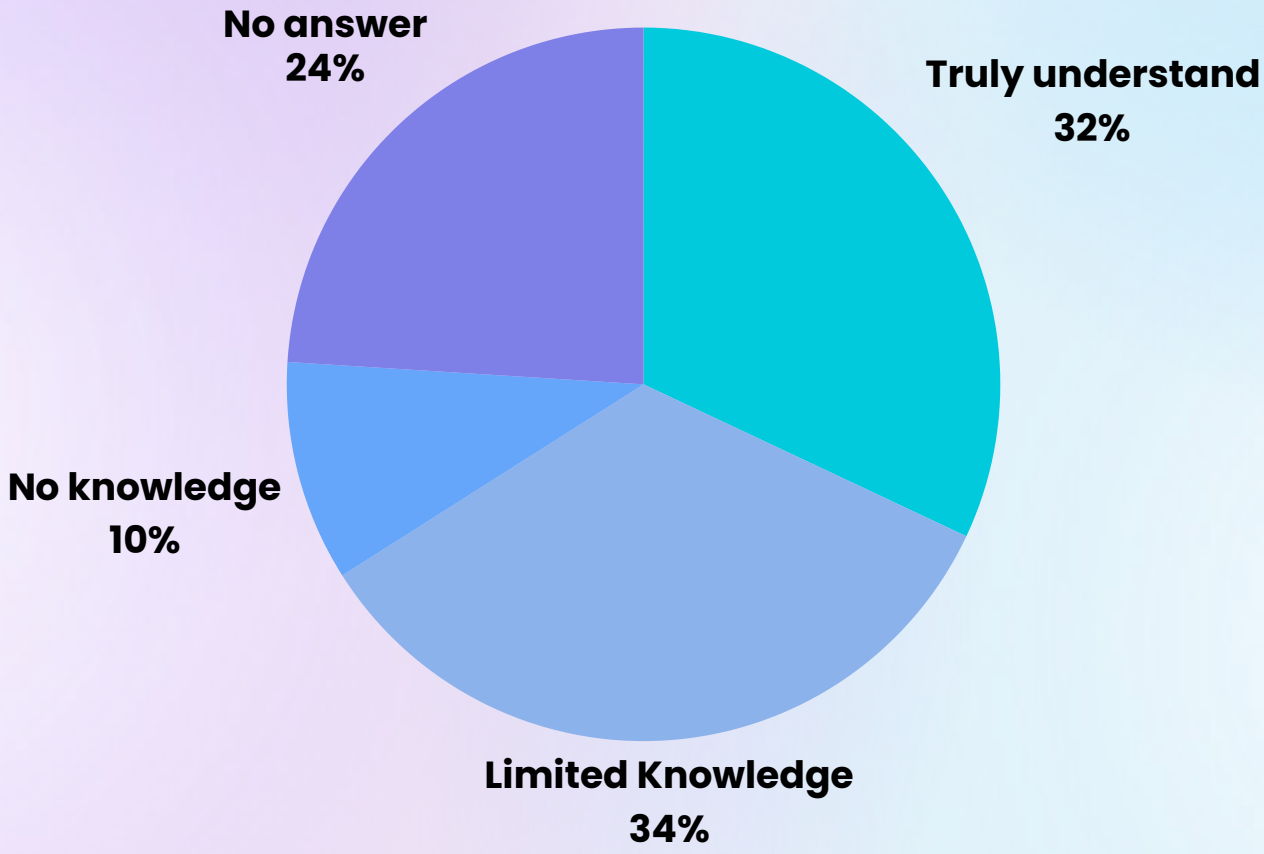
In Türkiye, awareness was broader, with 75% reporting general or partial knowledge, but much of this confidence was partial rather than deep. Both cases highlight the gap between awareness and practice: Romanian youth often recognize cybersecurity risks but feel underprepared, while Turkish youth show greater awareness yet lack consistent skills to apply it effectively.

For the Erasmus+ project, this suggests that training should be adapted as a bilateral solution to help each context and prepare the youth in a non-formal manner, including elements of theory but most of practice through gamification.

Co-funded by the European Union

CYBERSECURITY AWARENESS LEVEL

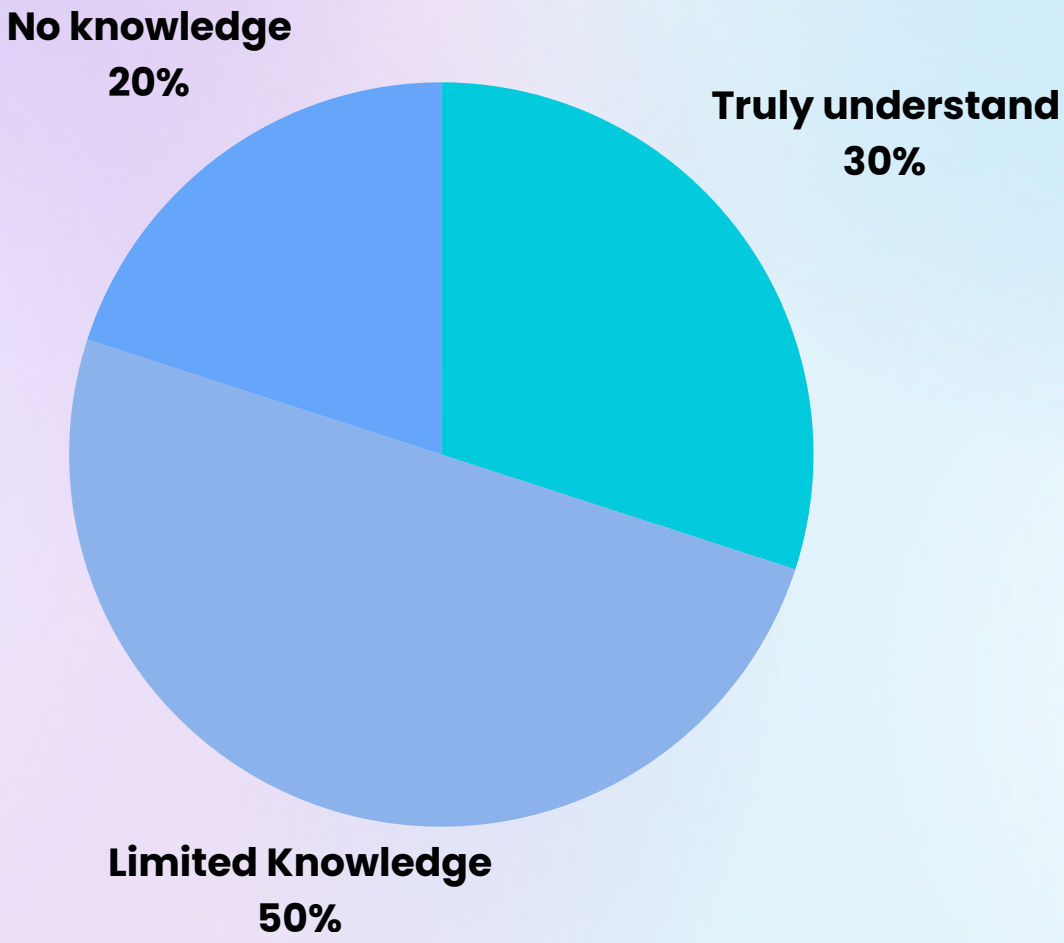
Türkiye



Co-funded by the European Union

Türkiye	Romania	Total Participants
187	153	340

Romania



Co-funded by the European Union

SAFETY / PROTECTIVE ONLINE BEHAVIORS

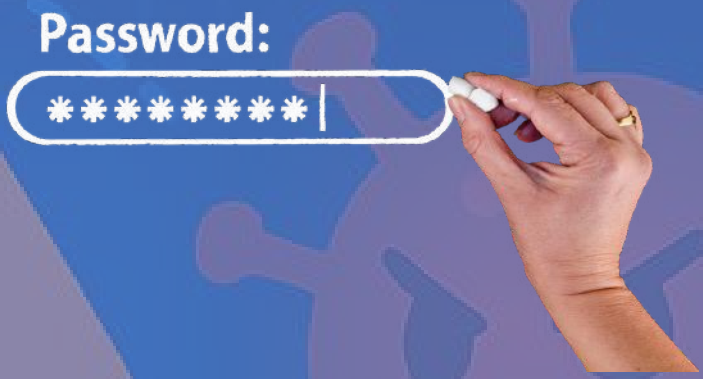
Romania

Romanian participants reported some awareness of safe online practices, but their behaviors reveal important gaps. Nearly all claimed to use strong passwords, and two-factor authentication is familiar to many, though not always consistently applied. Antivirus software was also widely used, but not universally, and some participants appeared to overestimate its effectiveness.

When it comes to online sharing, most participants—especially those from urban areas—reported being careful with what they post. Still, a minority admitted that they rarely adjust privacy settings or give little thought to personal information shared online.

Password management is a major weak spot. Only 32% reported using password managers, while 68% admitted to reusing the same password across accounts or storing them insecurely (e.g., written on paper or in phone notes). App downloads were largely from official sources, which is positive, but almost no participants read privacy policies, with most simply clicking through. Awareness of advanced privacy practices was limited, with only 35% reporting awareness. In summary, Romanian participants show a foundation of basic cybersecurity habits but remain vulnerable in areas like password management, privacy settings, and critical digital literacy.

Co-funded by
the European Union



Türkiye

Turkish participants demonstrated stronger engagement with protective online behaviors, supported by quantitative results. 83.4% reported using strong passwords, and nearly half (49.7%) combined this with two-factor authentication, reflecting an awareness of layered protection. 56% used antivirus software, and 30.5% regularly updated software, signaling proactive habits against common threats. Additionally, 75.4% avoided suspicious links or emails, aligning with their awareness of phishing risks.

Social media behaviors showed moderate caution: 59.9% avoided sharing personal information, and 33.7% regularly reviewed privacy settings, though some still admitted to inattentive posting. When asked about risks, identity theft (39%) emerged as the most pressing concern. Password management practices were mixed: 47.6% used different passwords across accounts, yet 21.4% still reused passwords. Only 18% used password managers, and some relied on insecure storage methods. App usage was mostly responsible, with 66.3% downloading from official app stores. Engagement with privacy policies was limited: about half read them occasionally, 26% never, and only 24% consistently reviewed them. Encouragingly, 54% expressed interest in improving their cybersecurity knowledge, showing readiness for further education.

In summary, Turkish participants displayed relatively stronger cybersecurity practices than their Romanian peers, though issues like password reuse, infrequent software updates, and low engagement with privacy policies remain areas for improvement.

Co-funded by the European Union

COMPARATIVE ANALYSIS

Although Romanian participants showed weaker habits in areas such as password management and privacy, and Turkish participants displayed stronger practices but with inconsistent application, both groups share a common need: to move from basic awareness to confident, consistent, and practical digital safety skills. For this reason, a single training approach can effectively serve both contexts by combining foundational knowledge with hands-on practice. The training should include theory and practical exercise, especially non-formal and gamified, as they are addressed especially to the youth segment, on the following topics:

- Password security module: Teaching strong password creation, safe storage methods, and encouraging the use of password managers.
- Two-factor authentication practice: Step-by-step exercises on enabling 2FA across popular platforms.
- Privacy awareness workshop: Demonstrating how to adjust privacy settings on social media and why privacy policies matter.
- Safe browsing and phishing simulation: Interactive activities where participants learn to spot suspicious links, fake messages, and malicious apps.
- Software and device hygiene: Emphasizing the importance of updates, antivirus use, and recognizing realistic limitations of protective software.

By focusing on applied exercises rather than just theory, this training would raise confidence among Romanian youth while reinforcing and deepening good habits already present in Turkish youth.

In short, a blended “digital safety toolkit” training—covering passwords, privacy, phishing, and device security—would ensure both groups are equally equipped to handle cybersecurity risks in daily life.

Co-funded by
the European Union

SAFETY/ PROTECTIVE ONLINE BEHAVIORS

Password habits:

- Romania: 68% reuse passwords, only 32% use password managers
- Türkiye: 47.6% use unique passwords, 21.4% reuse passwords, only 18% use password managers

Privacy and sharing:

- Romania: 35% aware of advanced privacy practices, many rarely adjust privacy settings
- Türkiye: 59.9% avoid sharing personal information, 33.7% regularly review privacy settings

Antivirus/software use:

- Romania: Common but not universal (majority use it, but some rely too much on it)
- Türkiye: 56% use antivirus, 30.5% update software regularly

Two-factor authentication:

- Romania: Known by many but inconsistently applied
(no clear % reported)
- Türkiye: 49.7% actively use it

Co-funded by the European Union

EXPERIENCE WITH CYBER ATTACKS

Romania

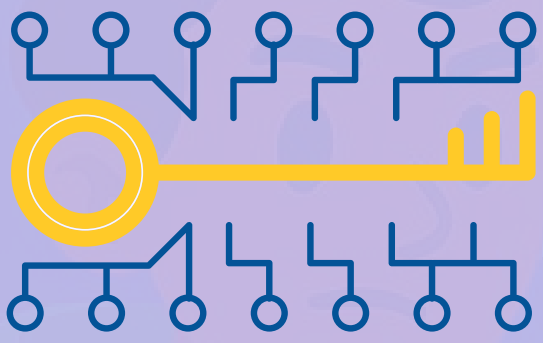
Among Romanian participants, few reported direct experiences with cyberattacks in the past year. The most frequently mentioned incidents involved phishing attempts, such as deceptive messages aimed at stealing account credentials, or unauthorized login attempts linked to weak or reused passwords.

Although actual account loss was rare, those who went through it described it as frustrating and memorable, underlining the emotional impact even a single breach can have. Additionally, a few rural participants noted that they did not feel targeted, either because they spend less time online or because they had not encountered any problems yet.

Overall, the findings suggest that everyday risks—especially phishing and poor password practices—pose the greatest threats for Romanian youth, even if some rural respondents perceive themselves as less exposed.

Türkiye

In Türkiye, only 9.1% of participants reported experiencing a cyberattack in the past year, while the majority (84.5%) stated they had not faced such incidents. A small proportion of respondents indicated that they could not recall if they had been affected.



Among the reported cases, the most common threat was attempted theft of personal or identity-related information, showing that attackers were primarily targeting sensitive data rather than spreading general malware. These findings emphasize that while direct attacks were not widespread, identity-related risks are a significant concern for Turkish youth.

Co-funded by
the European Union

COMPARATIVE ANALYSIS

Both Romanian and Turkish participants reported relatively low direct exposure to cyberattacks, though their experiences show some notable differences. In Romania, incidents were mainly phishing attempts or weak-password breaches, with rare but impactful cases of account loss. Rural participants often reported feeling less targeted, citing lower levels of online engagement. In Türkiye, 9.1% reported being attacked, most often through identity theft attempts, while the vast majority (84.5%) had not experienced cyberattacks.

Taken together, the results suggest that cyberattacks are not yet widespread among young people in either country, but the perceived risks differ: Romanian youth tend to connect threats to passwords and phishing, while Turkish youth express greater concern about identity theft and data protection.

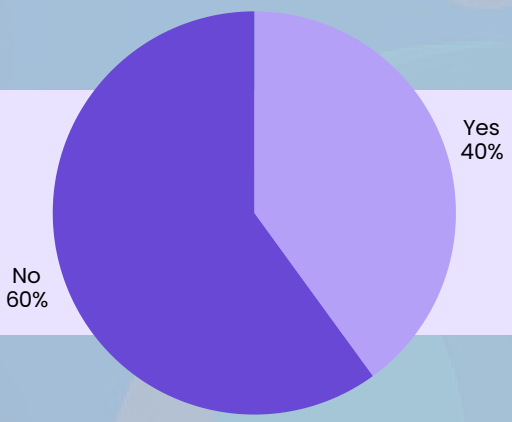
Training suggestion: A unified program should combine practical password hygiene exercises, phishing recognition simulations, and identity protection strategies, ensuring both urban and rural participants feel equally equipped to manage risks.

Co-funded by the European Union

EXPERIENCE WITH CYBER ATTACKS

Experience with Cyber Attacks in Türkiye

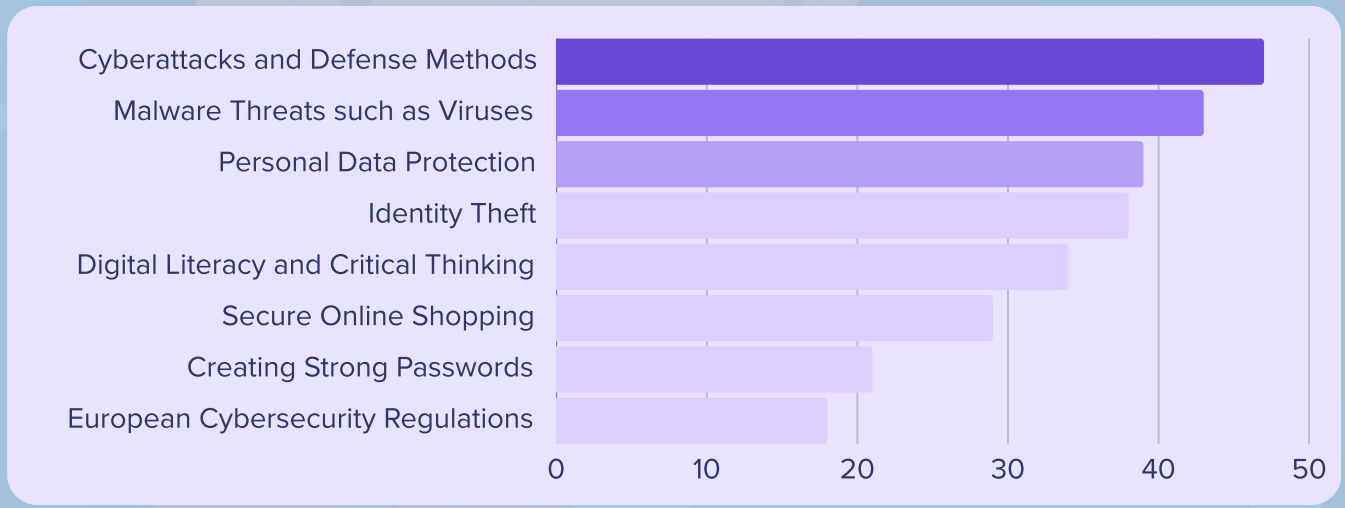
Experience with Cyber Attacks in Romania



*based on 340 responders

Co-funded by
the European Union

Interest in Cybersecurity Education in Türkiye

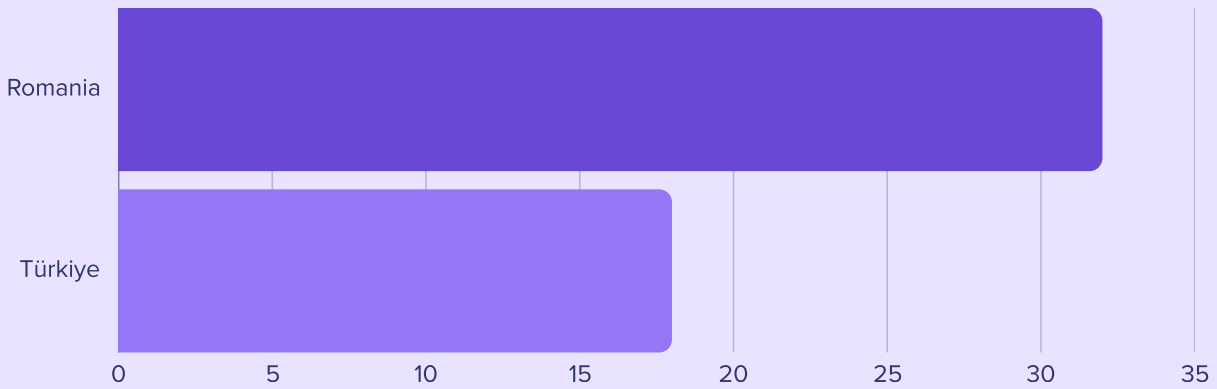


*based on 340 responders

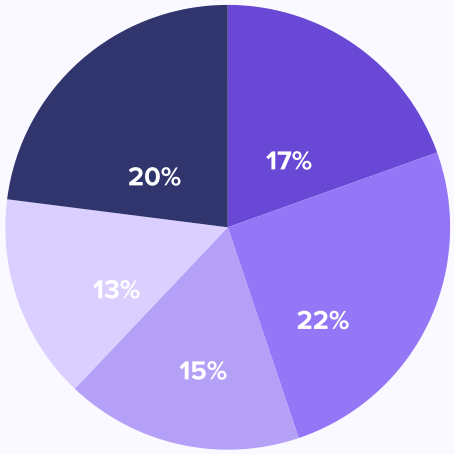
Co-funded by the European Union

SAFETY/PROTECTIVE ONLINE BEHAVIORS

Using Password Managers

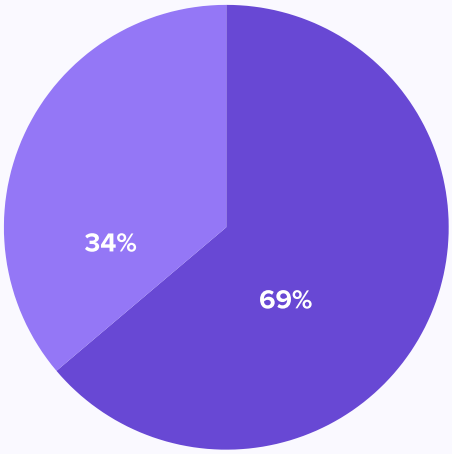


Cybersecurity Practices Among Participants in Türkiye



- Two-factor Auth.
- Official App sources
- Reliable Antivirus prog.
- Strong Password
- Avoid Suspicious Links

Social Media Behaviors in Türkiye



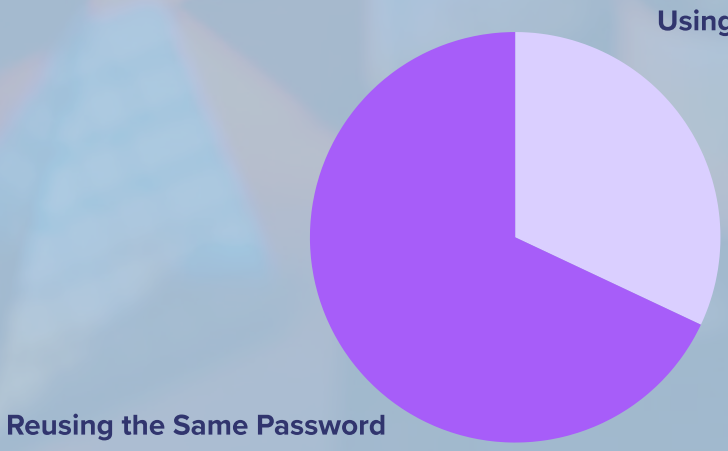
- Avoid Sharing Personal Information
- Regularly Reviewed Privacy Settings

*based on 340 responders

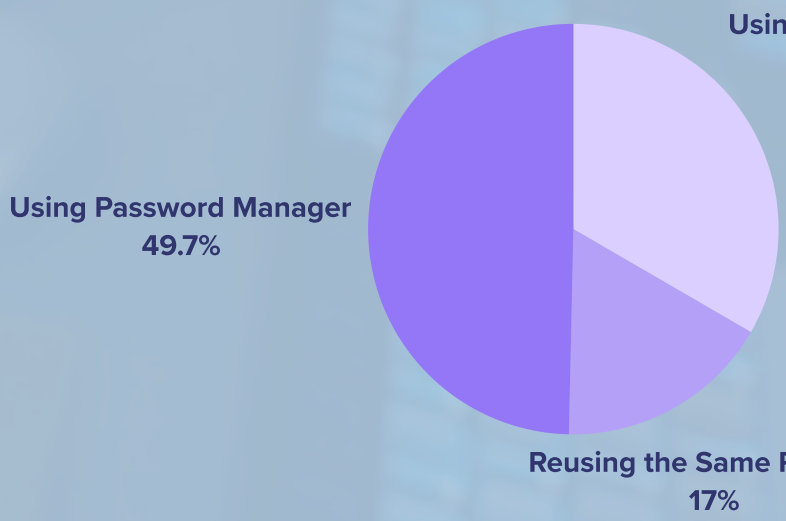
Co-funded by
the European Union

SAFETY/PROTECTIVE ONLINE BEHAVIORS

Password Management in Romania



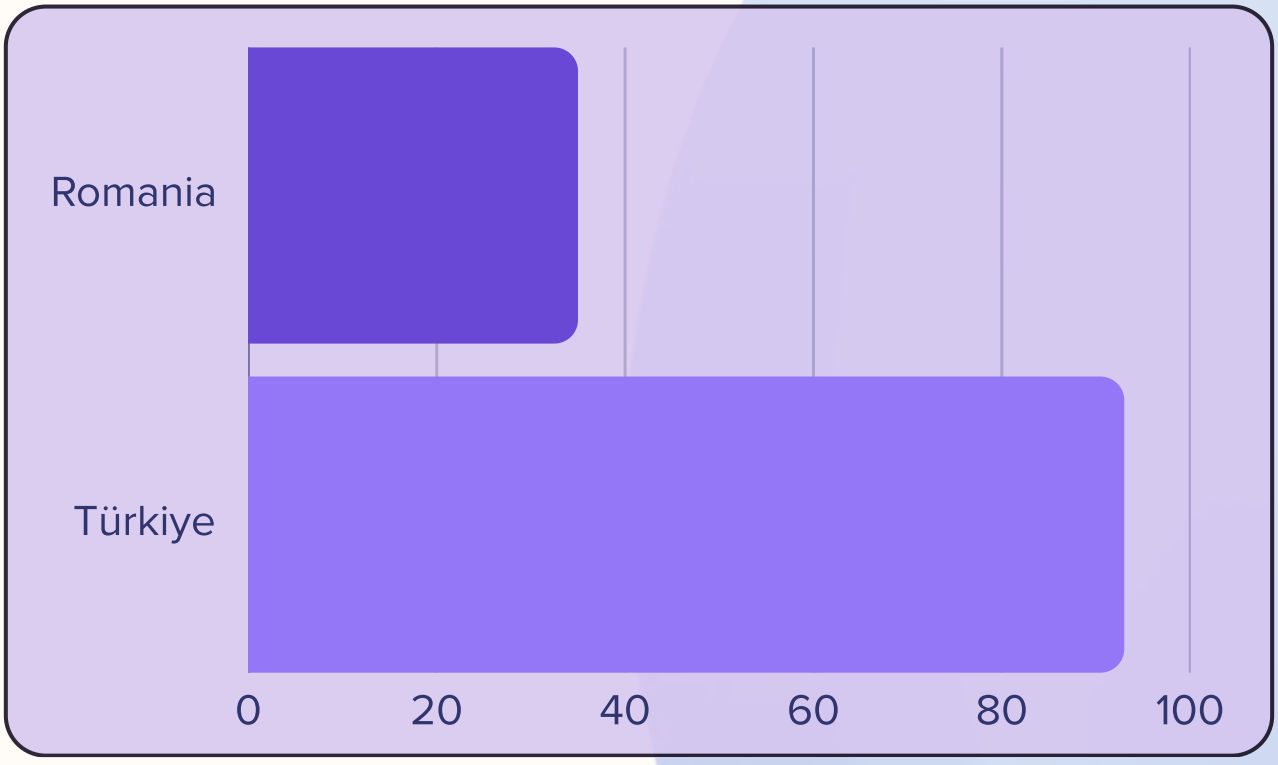
Password Management in Türkiye



Co-funded by
the European Union

SAFETY/PROTECTIVE ONLINE BEHAVIORS

Privacy and sharing



*based on 340 responders

Co-funded by
the European Union

KEY INSIGHTS, OBSERVATIONS, AND RECOMMENDATIONS

Romania

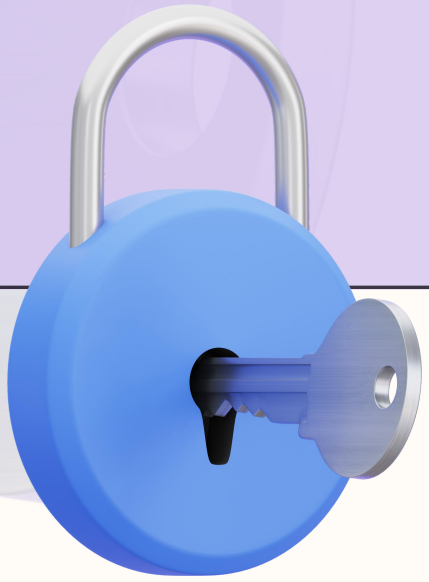
The Romanian results highlight a clear gap between knowledge and behavior. Many participants could list good cybersecurity habits in theory, but admitted to not applying them consistently. Common issues included reusing passwords, ignoring software updates, or placing excessive trust in antivirus software.
Direct quotes illustrate these tendencies:

"I have antivirus, so I don't worry much about anything else."
"Honestly, I never read privacy policies. Too long."

Urban youth generally showed slightly greater caution than rural peers, especially regarding online sharing and privacy settings. However, risky shortcuts and unsafe practices were present across both groups.

Türkiye

In Türkiye, no major inconsistencies were identified in the responses. Since the majority of participants were very young, the topics they emphasized were fairly typical, focusing on phishing, passwords, and data protection. Most participants demonstrated a solid awareness of password safety, and no unusual behaviors or unexpected personal notes emerged from their responses.



Co-funded by the European Union

COMPARATIVE ANALYSIS

The Romanian and Turkish groups both reflected typical youth cybersecurity concerns, but their overall approaches differed slightly.

Romanian youth often showed a gap between what they know and what they do, admitting to risky behaviors such as password reuse or ignoring privacy policies, even while recognizing these as unsafe. Their responses revealed a certain overreliance on antivirus software and a tendency to prioritize convenience over security.

Turkish youth, by contrast, presented a more consistent alignment between awareness and behavior, with most demonstrating solid basic knowledge and no notable contradictions in their answers. Their concerns remained typical for their age group, centered on phishing, passwords, and data protection.

In summary, while both groups are aware of key digital risks, the Romanian participants struggle more with turning awareness into action, whereas Turkish participants appear more consistent in applying basic practices, though their focus remains largely at the level of fundamental online threats.

CONCLUSIONS

Romania

The findings from the Romanian group show that youth are aware of digital risks, but this awareness does not always translate into consistent protective behaviors. While most participants reported taking some precautions, risky shortcuts—such as reusing passwords, relying too heavily on antivirus software, or ignoring privacy policies—remain widespread. The positive side is that these young people are eager to learn more and clearly motivated to improve their cybersecurity practices. Their strong interest in practical, hands-on advice suggests that with the right resources, it is possible to close the gap between knowing and doing, equipping them with the skills and confidence needed to stay safe online.

Türkiye

The Turkish results reveal a similar pattern: while participants demonstrated a foundational awareness of cybersecurity, important gaps remain in phishing recognition, password management, and privacy literacy. Their overall behaviors indicate a generally cautious attitude, but password reuse and skipping privacy policies continue to present risks. Across the group, participants expressed a high level of interest in improving their digital safety, with consistent preferences for practical skills such as protecting personal data and identifying scams.

Co-funded by the European Union

COMPARATIVE & PROJECT-LEVEL CONCLUSION

Romania

The findings from the Romanian group show that youth are aware of digital risks, but this awareness does not always translate into consistent protective behaviors. While most participants reported taking some precautions, risky shortcuts—such as reusing passwords, relying too heavily on antivirus software, or ignoring privacy policies—remain widespread. The positive side is that these young people are eager to learn more and clearly motivated to improve their cybersecurity practices. Their strong interest in practical, hands-on advice suggests that with the right resources, it is possible to close the gap between knowing and doing, equipping them with the skills and confidence needed to stay safe online.

Türkiye

The Turkish results reveal a similar pattern: while participants demonstrated a foundational awareness of cybersecurity, important gaps remain in phishing recognition, password management, and privacy literacy. Their overall behaviors indicate a generally cautious attitude, but password reuse and skipping privacy policies continue to present risks. Across the group, participants expressed a high level of interest in improving their digital safety, with consistent preferences for practical skills such as protecting personal data and identifying scams.

Co-funded by
the European Union

For our Erasmus+ project, this means that a unified training framework —built around interactive methods, gamification, and applied skills—can effectively address the needs of youth in both countries.

By moving beyond abstract theory and into real-world practice, the project can help close the gap between awareness and action, ensuring that participants are not only informed but also empowered to protect themselves online.

Co-funded by
the European Union

RESEARCH REPORT

CYBERESCAPE

Funded by the European Union. Views and opinions expressed are those of the author(s) and do not necessarily reflect the views and opinions of the European Union, the European Education and Culture Executive Agency (EACEA) or ANPCDEFP. The European Union, the EACEA or ANPCDEFP cannot be held responsible for them.