



ESCAP(E+)

**Educate Youth in Security through Cyber
Awareness Program and Engagement**

DESK RESEARCH



Co-funded by
the European Union

Project & Contributors

This Desk Research report has been developed as part of the “ESCAP(E+) Educate Youth In Security Through Cyber Awareness Program And Engagement”

Project Number: 2025-1-ES02-KA220-YOU-000358192

Publication Date: 1 April 2026

Partners and Contributors:

Suatas Project Academy SPA - Lithuania
info@suatasprojectacademy.lt

EducAI - Portugal
educai.ngo@gmail.com

EducPro Spain
projects@educpro.eu

EuroReach - Estonia
info@euroreach.org

Istanbul University-Cerrahpasa - Turkiye
irfan@iuc.edu.tr

Scout Society - Romania
contact@scoutsociety.ro

This project has been funded with support from the European Commission. This document reflects the views only of the author(s), and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Agreement number: 2025-1-ES02-KA220-YOU-000358192

Acknowledgement

This Desk Research Report has been developed as part of the ERASMUS+ Cooperation Partnership in the youth project “ESCAP(E+) Educate Youth In Security Through Cyber Awareness Program And Engagement” funded by the European Commission under Grant Agreement number 2025-1-ES02-KA220-YOU-000358192. The project has a duration of 24 months, from 1 December 2025 to 30 November 2027, and this publication was released on 1 April 2026.

This project was made possible through the collaborative efforts of our partners:

- EducPro(SP)
- EuroReach (EE)
- Istanbul University-Cerrahpasa (TR)
- Scout Society Association (RO)
- Suatas Project Academy SPA (LT)
- EducAi (PT)

Special thanks to the partners, researchers, youth workers, and contributors who supported the desk research process.

Disclaimer

The European Commission's support for the production of this publication does not constitute an endorsement of the content, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Copyright notice

This license allows users to distribute, remix, adapt, and build upon the material in any medium or format for noncommercial purposes only, provided that attribution is given to the original source. Any adaptations must be shared under the same license terms.

If you use or adapt content from this publication, please include the following statement:

"This content has been developed using materials from the ESCAP(E+) project (Project Number:2025-1-ES02-KA220-YOU-000358192). All visuals used in this publication are copyright-free and sourced from Canva.

Contents

5	Introduction
7	Desk Research Lithuania
15	Desk Research Romania
32	Desk Research IUC
46	Desk Research Estonia
66	Desk Research Spain
79	Desk Research Portugal
92	Conclusion

INTRODUCTION

This desk research was developed within the ESCAP(E+) project Work Package 2: Framework – Exploring Cyber Security Threats, led by Suatas Project Academy. Its purpose is to identify and analyse the most relevant cybersecurity threats affecting young people, especially those appearing on widely used digital platforms such as Facebook, Instagram, TikTok, and email. In the wider logic of the project, this research provides the evidence base for the development of the ESCAP(E+) cybersecurity framework and supports the creation of later project outputs, including training content for youth workers, VR escape game scenarios, awareness materials, and other educational resources.

The report was prepared through a coordinated, partner-based desk research process. Following a shared methodology agreed within WP2, each partner conducted national research using a common template in order to ensure consistency and comparability across countries. Partners were asked to focus on youth digital habits, key risk factors, the most common online threats, and available prevention and reporting mechanisms in their national context. To make the findings practical and usable, each partner described key threats through a standard structure that included the platform concerned, a short description of the threat, a realistic youth scenario, how the threat works, red flags, prevention tips, response steps, severity, and key sources.

This report, therefore, combines the national contributions of all partners into one consolidated document. It includes an overview of the youth digital context in each partner country, a presentation of the most relevant cyber threats targeting young people, and practical guidance on prevention and response. In this way, the report helps ensure that the ESCAP(E+) project is rooted in real youth experiences, reflects country-specific risks, and responds to the actual educational needs of young people and those who work with them.

METHODOLOGY

Each partner was asked to carry out national-level desk research in its own country context and then submit its findings in the shared format so that the results could be consolidated into one comparative project report. This common approach made it possible to combine country-specific evidence while maintaining consistency across the full document.

For the national reports, partners followed a shared structure composed of four main sections: **Overview, Key Threats, Conclusions, and Resources**. The overview section introduced the national context, including youth digital habits, key vulnerabilities, selected statistics, and reporting channels. The research focused on the digital environments and cyber threats that are most relevant to youth in everyday life. In line with the project framework, partners were asked to examine risks connected to widely used platforms and communication channels, especially **Facebook, Instagram, TikTok, and Email**, including threats such as phishing, scams, identity theft, misinformation, impersonation, and other forms of social engineering. In addition to mapping the threats themselves, partners also examined the broader youth digital context in their countries, including online habits, platform use, common vulnerabilities, and available support or reporting mechanisms.

A further strength of the methodology is that it combines country-specific relevance with project-level coherence. Each partner was able to identify the scams, manipulation tactics, and digital risks that are most visible in its own national setting, while the use of a shared template ensured that all contributions could be compared, merged, and translated into common project recommendations. As a result, the final report not only describes threats in abstract terms, but links them to the daily digital realities of young people across the partner countries.



ESCAP(E+)

Lithuania

DESK RESEARCH



Co-funded by
the European Union

Project funded by the European Union
under the Erasmus+ programme

Overview

Youth Digital Context in Lithuania

In Lithuania, digital integration is among the highest in the European Union. As of 2026, national statistics indicate that 99.2% of individuals aged 16–24 are daily internet users (Statistics Lithuania, 2026). Digital tools are essential for the "e-resident" lifestyle common in the Baltics, with youth utilizing high-speed 5G networks for social media (TikTok, Instagram), academic research, and government services. For the majority of Lithuanian youth, the smartphone is the primary device for identity verification via Smart-ID or Mobile-ID, which are integrated into nearly all aspects of life (National Cyber Security Centre [NCSC], 2025).

Key Risk Factors

Despite high technical proficiency, a "trust gap" exists regarding social engineering. Many young users, particularly international students and job seekers, demonstrate a high level of trust in "community" environments such as Facebook Groups (NCSC, 2025). The intensive use of automated authentication tools (Smart-ID) can sometimes lead to "authentication fatigue," where users approve push notifications without critical evaluation, facilitating unauthorized account access (Communications Regulatory Authority [RRT], 2026).

Support and Reporting Channels

Lithuania provides several robust channels for cyber assistance. The National Cyber Security Centre (NCSC) serves as the primary technical authority. For fraud and identity theft, the Lithuanian Police operate the epolicija.lt portal for formal reporting. Additionally, the Saugus Internetas initiative provides educational resources and a helpline specifically tailored for youth and educators (Saugus Internetas, 2026).

Facebook Threat

Anonymous Recruitment & Data Harvesting



Main Platform

Facebook Groups (e.g., "Foreigners in Vilnius," "Jobs for Students")



Short Description

Scammers exploit the "Anonymous Member" feature to post fraudulent job openings. They target youth by offering "low-threshold" remote work to collect photos of ID cards and Residence Permits for identity theft (NCSC, 2025)



Typical Youth Scenario

A student sees an anonymous post for a "Social Media Assistant." After a brief Messenger chat, the "employer" asks for a photo of their ID to "check work rights in the EU." Once the photo is sent, the user is blocked, and their ID is used to open a neobank account (Lietuvos Policija, 2026)



How does it work?

- Scammer posts a high-paying job anonymously.
- Moves conversation to private, encrypted apps.
- Requests sensitive documents (ID/Passport) immediately.
- Victim is blocked and data is sold on the dark web.



Red Flags

- Use of "Anonymous Member" status for job postings.
- Requests for personal documents before an official contract or interview.
- Salary offers that far exceed the average Lithuanian student wage.



Prevention Tips

- Never share ID photos via social media chats.
- Verify the existence of the company via Rekvizitai.lt.
- Demand a video interview or an in-person meeting at a registered office.



What to do if it happens?

- Immediately report the theft of data at epolicija.lt.
- Contact your bank to warn of potential identity impersonation.
- Alert the group moderators to remove the post.



Severity

Likelihood 5/5 – This is the most prevalent social engineering threat in Lithuanian expat and youth circles in 2026 (NCSC, 2025).



Key Sources

NCSC (2025); Lietuvos Policija (2026)

Instagram Threat

Job Scams / Recruitment Fraud



Main Platform

Instagram



Short Description

"Recruitment fraud" on Instagram has become a relevant threat for young people in Lithuania. Scammers impersonate HR staff, recruiters, or representatives of well-known companies and use direct messages or sponsored-looking posts to offer fake job opportunities. Their goal is usually to collect personal data, copies of identity documents, banking details, or small "onboarding" or "processing" fees.



Typical Youth Scenario

A university student or recent graduate in Lithuania sees an Instagram post promoting a flexible remote job with attractive pay. After liking or following the page, they receive a direct message from an account claiming to represent a well-known company. The "recruiter" asks them to continue the application quickly by sending a CV, ID details, and bank account information, or by paying a small fee for training materials or contract processing. After the data or payment is sent, the account disappears or continues the scam using the victim's information.



How does it work?

- A scammer creates a fake company or recruiter profile using a copied logo, job graphics, and professional-looking posts.
- They target young people through Instagram posts, stories, ads, or direct messages offering part-time, remote, or student-friendly jobs.
- The scammer creates urgency by saying the vacancy is limited or the application must be completed immediately.
- The victim is asked to provide personal documents, contact details, banking information, or a small payment for "registration," "training," or "onboarding."
- Once the data or money is received, the scammer blocks the victim or uses the information for identity theft or further fraud.

Instagram Threat

Job Scams / Recruitment Fraud



Red Flags

- The recruiter contacts the user unexpectedly through Instagram DMs.
- The account has few followers, little real interaction, or was created recently.
- The job offer promises very high income for simple work.
- The recruiter asks for ID copies, bank details, or payment at an early stage.



Prevention Tips

- Verify the company through its official website and official contact channels.
- Never send ID documents, bank details, or personal codes through Instagram chat.
- Do not pay any fee to access a job offer, training, or recruitment process.
- Ask for a formal email from the company domain and request a real interview.



What to do if it happens?

- Stop communication immediately and do not send any more information or money.
- Save screenshots of the account, messages, job offer, and any payment request.
- If personal data or ID documents were shared, report the incident to the Lithuanian Police via epolicija.lt.
- If banking details were shared or a payment was made, contact the bank immediately.
- Report the scam to the National Cyber Security Centre and seek guidance through national online safety channels.



Severity

Likelihood 4/5 – This threat is highly relevant for students, recent graduates, and young job seekers because Instagram is widely used for networking, side jobs, and digital opportunities, and scammers exploit trust in familiar brand identities.



Key Sources

- National Cyber Security Centre (NCSC)
- Lietuvos Policija
- Saugus Internetas
- Communications Regulatory Authority (RRT)

TikTok Threat

Live Stream & Celebrity Giveaway Fraud



Main Platform

Tiktok



Short Description

Scammers use looped, high-quality video clips of popular influencers or celebrities to host "Live" events. They trick youth into paying "verification fees" or entering bank details to win prizes (Saugus Internetas, 2026).



Typical Youth Scenario

A teen joins a "Live" stream of a famous gamer. A bot-driven chat claims they won an iPhone but must pay a 10€ "customs fee" via a link in the bio. The teen pays, but the link is a phishing site that drains their card.



How does it work?

- A scammer streams a stolen video of a celebrity.
- Fakes "Live" viewer numbers to build credibility.
- Directs users to a phishing link to "claim" rewards.
- Collects credit card info or Smart-ID logins.



Red Flags

- The "Live" video is low resolution or obviously looped.
- The account handle is a variation of a real name (e.g., @FamousStar_LT_Official).
- Requirement of any payment for a "free" prize.



Prevention Tips

- Check for the official blue verification badge.
- Look at the "About this account" section to see the account's history.
- Never provide card details to "claim" a prize.



What to do if it happens?

- Freeze your bank card immediately via your mobile app.
- Report the stream for fraud to the platform.
- Inform the NCSC about the malicious URL.



Severity

Likelihood 4/5 – Highly effective among younger adolescents who follow trending influencers (RRT, 2026).



Key Sources

Saugus Internetas (2026); Meta Security Alerts (2025).

Email Threat

QR Code Phishing (Quishing)



Main Platform

E-Mail



Short Description

Malicious emails impersonate Lithuanian institutions (e.g., VMI or Sodra) using QR codes to bypass email filters. These codes lead to fake login portals designed to steal Smart-ID credentials (NCSC, 2025).



Typical Youth Scenario

A university student receives an email regarding a "VMI Tax Refund." Instead of a link, it shows a QR code to "Scan for Smart-ID Login." The student scans it, enters their PINs on a fake site, and their bank account is accessed (VMI, 2026).



How does it work?

- Scammer sends a high-urgency email with a QR code.
- The code bypasses security software that only scans text links.
- User scans with a phone, opening a phishing site.
- User provides Smart-ID/banking credentials.



Red Flags

- Use of a QR code as the only way to log in.
- Sender email address is not from a .gov.lt or .vmi.lt domain.
- Language that pressures the user to act within minutes.



Prevention Tips

- Always log in to state portals directly (vmi.lt, sodra.lt).
- Use a QR scanner that previews the destination URL.
- Be wary of any email asking for Smart-ID authentication.



What to do if it happens?

- Revoke your Smart-ID certificates immediately.
- Contact your bank's emergency line.
- Report the email to cert@nksc.lt.



Severity

Likelihood 4/5 – A rapidly growing threat in 2026 as scanners become more adept at bypassing traditional filters (NCSC, 2025).



Key Sources

VMI (2026); NCSC (2025).

Conclusions

The findings indicate that Lithuanian youth are increasingly targeted by "platform-specific" scams that exploit the local digital infrastructure (Smart-ID and Facebook community trust). These threats are relevant because they mirror the daily habits of youth: seeking employment, engaging with influencers, and managing state services online.

Application for ESCAP(E+) Project:

Training Guidance: Focus on "Visual Literacy"—recognizing deepfake "Live" streams and fraudulent "Anonymous" posts.

VR Scenarios: Create an immersive "Digital VMI Office" where players must distinguish between a real QR login and a phishing attempt.

Awareness Content: Distribute infographics that highlight the legal requirement for Lithuanian employers to be registered on Rekvizitai.lt.

Resources

- Communications Regulatory Authority [RRT]. (2026). Report on the digital habits and safety of Lithuanian youth. <https://www.rrt.lt>
- Lietuvos Policija. (2026). Cybercrime and fraud prevention guidelines for 2026. <https://policija.lrv.lt>
- National Cyber Security Centre [NCSC]. (2025). Lithuanian cyber security status report: Social engineering trends. <https://www.nksc.lt>
- Saugus Internetas. (2026). Youth online safety and reporting protocols. <https://www.saugusinternetas.lt>
- Statistics Lithuania. (2026). Information society in Lithuania: Usage of ICT by age group. <https://osp.stat.gov.lt>
- State Tax Inspectorate [VMI]. (2026). Security notice regarding phishing and fraudulent QR codes. <https://www.vmi.lt>



ESCAP(E+)

Romania

DESK RESEARCH



Co-funded by
the European Union

Overview

Youth digital habits (main platforms & typical use)

In Romania, internet use among teenagers is close to universal and strongly daily-habit based: a recent national study reports that 95.7% of high-school students use the internet every day, and that students mainly use it to communicate on social media and consume content on social platforms, often consuming more than they create. This makes TikTok, Instagram, YouTube and messaging (Messenger/WhatsApp) central to how young people socialize, follow trends, discover opportunities (events, jobs, scholarships), and shape identity. The same consumption-heavy pattern also creates a fast spread environment for viral misinformation, risky challenges, and scam funnels(links in bio, Telegram/WhatsApp redirects, “giveaways”, fake forms).

Key risk factors/vulnerabilities in Romania

Romania’s youth online safety challenges are shaped by early entry into social media, very high screen time, and social pressure dynamics that spill over from school into online spaces:

High exposure time & early access

A 2025 Save the Children Romania study (as reported by Agerpres) indicates that 48.3% of children spend more than 6 hours/day in the digital environment, with much of that time on social media. Long exposure increases contact with strangers, visibility of harmful content, and the likelihood of impulsive sharing or clicking.

Cyberbullying, harassment, shame-based attacks (often school-linked)

EU Kids Online’s Romania country profile notes that children’s negative online experiences increased (e.g., 33% in 2018 vs 21% in 2010) and describes cyberbullying patterns (witnessing bullying rises with age; girls often report being more bothered by it).

Overview

In practice, this often appears through “confessions/exposure” pages, screenshot-sharing, rumor piles-on, and coordinated harassment between classmates.

Fraud, impersonation and “instant payment” exploitation

Romanian youth are exposed to scams that exploit trust and speed: hacked-account “urgent money” requests, fake giveaways, Marketplace/courier payment links, or phishing disguised as tickets/jobs/scholarships. These typically move users from TikTok/Instagram into Telegram/WhatsApp, then to short links or cloned forms, where personal data or payment details are harvested.

Misinformation and influence operations in short-video ecosystems

High reliance on social feeds for news/updates increases vulnerability to misleading content, especially when the platform rewards emotional or sensational clips and when verification is rare.

Main support/reporting channels in Romania

DNSC (Romanian National Cyber Security Directorate): national authority with PNRISC (National Cybersecurity Incident Reporting Platform) for reporting incidents; DNSC also lists phone 1911 (accessible from Romania) and the PNRISC link on its official contact page.

Telefonul Copilului – 116 111: free support line for children/adolescents (including bullying/abuse, mental health stressors and online harms); also runs cyberbullying prevention initiatives.

Police reporting: for cybercrime cases (fraud/blackmail/identity theft/sextortion), victims can file complaints via Romanian Police channels (local units/cybercrime structures).

Facebook Threat

Fake “Student Rent” listings & advance payment



Main Platform

Facebook



Short Description

Fake landlords post attractive rentals in university/high-school city groups, ask for advance payment to “secure the room” and send convincing but forged contracts/IDs. After payment, the listing disappears and the profile blocks the victim



Typical Youth Scenario

A first-year student (or a high-school graduate moving to a university city like Bucharest, Cluj, Iași or Timișoara) joins Facebook rental groups to find accommodation quickly before the academic year starts. They find an apartment that looks perfect—good photos, central location, “close to campus,” and a price below market. The “landlord” says there are many interested people and asks for a small advance payment (deposit) to reserve the room, sending a convincing-looking ID photo and a simple “contract” to build trust. After the transfer is made (often via instant bank transfer or Revolut), the listing disappears, the profile blocks the student, and the phone number stops responding.



How does it work?

- A scammer posts an attractive “student rent” listing in Romanian Facebook housing groups (often in big university cities).
- The price is usually below market and the photos/description look professional (sometimes copied from real listings).
- The scammer quickly moves the conversation to private messages or WhatsApp and creates urgency (“many interested”, “first to pay reserves it”).
- They send “proof” to look legitimate: a forged/edited ID photo, a fake contract, or a short video of the apartment (stolen from elsewhere).
- They refuse an in-person viewing and give excuses (out of town, key at a neighbour, current tenant still inside).
- They request an advance payment (reservation fee/deposit/first month) via instant transfer or Revolut to “secure the room”.
- Once the money is sent, the listing is deleted, the victim is blocked, and all communication stops.

Facebook Threat

Fake “Student Rent” listings & advance payment



Red Flags

- Price is noticeably below market for a popular area (“too good to be true”).
- The “landlord” pushes urgency: “many people interested”, “pay today or it’s gone”.
- Refuses a viewing (in-person or real-time video) or gives constant excuses (out of town, keys not available).
- Insists on advance payment before any visit (reservation fee/deposit/first month).
- Wants payment only via instant transfer / Revolut and avoids traceable contracts or official channels.
- Sends ID/contract photos that look edited (blurred text, mismatched names, inconsistent fonts, missing details).
- The profile looks suspicious: new account, few friends, stock photos, inconsistent activity, or copied posts.
- Communication style is inconsistent (copy-paste answers, avoids specific questions about utilities, lease terms, or neighborhood).



Prevention Tips

- Always insist on an in-person viewing, or at minimum a live video call where the landlord shows the apartment in real time (including the street view, entrance, and key details inside).
- Never send an advance payment to “reserve” a place before you have verified the property and the landlord’s identity.
- Ask for clear, consistent proof of ownership or the right to rent (e.g., ownership documents) and cross-check names across documents; be cautious if documents look edited or unclear.
- Use a written contract with complete details (full address, tenant/landlord ID details, rent, deposit, utilities, payment method) and do not rely on screenshots or “templates” sent over chat.
- Pay only through traceable methods after signing and after verification; avoid pressure to use instant transfers.
- Check the landlord profile carefully (account age, activity history, mutual friends, consistency of posts) and be cautious with newly created or “empty” profiles.
- Use reputable rental platforms or agencies when possible, and report suspicious listings to Facebook group admins and the platform.

Facebook Threat

Fake “Student Rent” listings & advance payment



What to do if it happens?

- Stop all communication and do not send any additional money, even if the scammer promises a refund.
- Collect and save evidence immediately: screenshots of the listing, profile details, chat messages, phone numbers, bank/Revolut details, receipts, and any documents they sent.
- Report the profile and the listing to Facebook, and inform the group admins so it can be removed and others warned.
- Contact your bank/payment provider as soon as possible to request a recall/chargeback and to flag the recipient account as fraudulent (success depends on timing, so act fast).
- If you shared card details, block the card and request a replacement; monitor your accounts for unauthorized transactions.
- File a police report in Romania and provide all evidence and payment details, especially the beneficiary account/IBAN and transaction reference.
- If you shared personal documents (ID/CNP), monitor for identity misuse, consider informing your bank and mobile provider, and be extra cautious with future verification requests or unexpected loans/subscriptions.
- Warn friends/classmates in the same housing groups so the scam doesn't spread, but avoid posting sensitive details publicly (share them only with admins/police/bank).



Severity

High severity, because victims can lose significant amounts of money quickly (deposit/advance rent), and if they share ID details or personal data, the scam can escalate into identity misuse and further targeted fraud.



Key Sources

Direcția Națională de Securitate Cibernetică (DNSC). (n.d.). Contact / support & reporting. <https://www.dnsc.ro/contact>
DNSC. (n.d.). National Cybersecurity Incident Reporting Platform (PNRISC). <https://pnrisc.dnsc.ro/>
SigurantaOnline.ro. (n.d.). What to do in case of online fraud. <https://sigurantaonline.ro/ce-fac-in-caz-de-frauda/>
Poliția Română. (n.d.). Online scam methods and spoofing attacks (guidance). <https://politiaromana.ro/ro/comunicate/metode-de-inselaciune-in-mediul-online-si-atacurile-de-tip-spoofing>

Instagram Threat

Brand Ambassador” scam targeting small creators



Main Platform

Instagram



Short Description

DMs offer ambassador deals (clothes, cosmetics, tech) and ask users to pay “customs/shipping” or log in to “brand portal.” Victims lose money, or their accounts get compromised and used for more scams.



Typical Youth Scenario

A teen or young adult with a small but active Instagram account (often posting fashion, gym, lifestyle or makeup content) receives a DM from a “brand” offering an ambassador deal and free products. The message looks professional and includes a link to a “brand portal” or a request to pay a small shipping/customs fee. Excited to collaborate, the creator either pays the fee or logs in via the link, after which money is lost and/or the Instagram account gets taken over and used to message friends with scams.



How does it work?

- A scammer creates a fake brand profile (logo, highlights, fake followers, and copied posts).
- They DM small creators in Romania with an “ambassador/collab” offer and promise free products + discount codes.
- They push urgency and exclusivity (“limited spots”, “reply today”).
- They ask for a “small fee” (shipping/customs/handling) paid via link, Revolut, or bank transfer, or they send a “brand portal” link.
- The payment link collects card data or triggers subscription fraud; the portal link is a phishing page that steals Instagram credentials (sometimes also 2FA codes).
- Once compromised, the victim’s account is used to scam followers (money requests, fake giveaways, phishing links).

Instagram Threat

Brand Ambassador” scam targeting small creators



Red Flags

- Brand contacts you out of the blue with a generic message and no real campaign details.
- They insist you must pay shipping/customs to receive “free” products.
- They send a suspicious link (shortened URL, odd domain, misspellings, non-official pages).
- They ask for your login details, 2FA code, or want you to “verify” via a login page.
- The brand profile looks artificial: recent account, repetitive posts, stolen photos, low engagement, weird follower patterns.
- They refuse a proper email contract/invoice and avoid giving a verifiable company address, VAT details, or official website.
- They pressure you with urgency or guilt (“we’ll pick someone else in 1 hour”).



Prevention Tips

- Verify the brand outside Instagram: official website, company details, independent reviews, and consistent contact info.
- Never pay “customs/shipping/handling” for a collaboration that claims to be free.
- Do not log in through links sent in DMs; access Instagram only through the official app/website.
- Check the sender profile carefully (account age, engagement, comments quality, tagged partners, real influencer collaborations).
- Ask for details that scammers usually can’t provide: written contract, campaign brief, official email domain, and legitimate invoice/shipping method.
- Enable strong security: unique password, two-factor authentication, login alerts, and review active sessions regularly.
- If you want to test legitimacy, suggest they email you from an official company domain; refuse personal Gmail/Yahoo “brand” emails.

Instagram Threat

Brand Ambassador” scam targeting small creators



What to do if it happens?

- Stop communicating and do not pay anything else.
- Screenshot everything: the DM, profile, links, payment requests, receipts, email addresses, and usernames.
- If you logged in via a link, immediately change your Instagram password and email password, revoke unknown sessions, and enable/refresh 2FA.
- Report the profile and messages to Instagram and warn your followers via story/post if your account was compromised.
- If you paid by card, contact your bank quickly to block the card and request a chargeback where possible; monitor transactions.
- If money was sent via Revolut/transfer, report it to the provider and file a police complaint with all evidence.



Severity

- Medium to high severity, because the scam can cause direct financial loss and can also escalate into account takeover, follower victimization, and reputational damage.



Key Sources

- Meta. (n.d.). Avoid scams and phishing on Instagram. <https://help.instagram.com/>
- Meta. (n.d.). Secure your Instagram account (security tips). <https://help.instagram.com/>
- Meta. (n.d.). Report abuse or suspicious content on Instagram. <https://help.instagram.com/>
- SigurantaOnline.ro. (n.d.). What to do in case of online fraud. <https://sigurantaonline.ro/ce-fac-in-caz-de-frauda/>
- Direcția Națională de Securitate Cibernetică (DNSC). (n.d.). Contact / support & reporting. <https://www.dnsc.ro/contact>
- DNSC. (n.d.). National Cybersecurity Incident Reporting Platform (PNRISC). <https://pnrisc.dnsc.ro/>

TikTok Threat

Fake “Contest / Talent Selection” with data & face capture



Main Platform

TikTok



Short Description

Clips promise casting for ads/music competitions and ask for short video submissions plus ID data “to prove age.” Collected videos and data can be reused for deepfake attempts, impersonation, or targeted scams.



Typical Youth Scenario

A teen who posts TikToks (dance, singing, comedy) sees a viral clip announcing a “casting” for an ad, music video, or “talent competition,” with prizes and “fast selection.” They are asked to submit a short video plus personal details to “prove age” (ID photo, full name, date of birth). Believing it’s a real opportunity, they send the materials via a form, email, or WhatsApp/Telegram, after which the data is reused for impersonation, harassment, or future scam targeting—and the video may later appear in deepfake content or fake accounts.



How does it work?

- Scammers post convincing casting/contest clips using logos, celebrity references, or “agency” language.
- They promise quick selection, paid gigs, or prizes and target teens/young creators in Romania.
- They direct users to submit entries via link-in-bio, Google Forms, email, or WhatsApp/Telegram.
- They request a short video showing face/voice plus “age verification” data (ID photo, date of birth, address, phone).
- Collected data is used to create fake profiles, attempt account recovery, or run tailored scams against the victim/family.
- Collected face/voice footage is repurposed for deepfake-style content, impersonation, or blackmail-style pressure.

TikTok Threat

Fake “Contest / Talent Selection” with data & face capture



Red Flags

- The “agency” has no verifiable website, official email domain, or company details (CUI/VAT/address).
- They ask for ID photos or sensitive data at the very first step “to prove age.”
- The submission method is informal or risky (Telegram/WhatsApp, random form links, personal email).
- Unrealistic promises: “guaranteed selection,” “instant payout,” “limited spots—apply in 1 hour.”
- The account is new, low engagement, copied content, or comments look artificial.
- They discourage parents/guardians or refuse to provide a written consent process for minors.
- They request extra videos with specific angles/phrases that feel like “data capture,” not casting.



Prevention Tips

- Treat any request for ID data as high-risk—real castings rarely need full ID at first contact; for minors, they should request parental/guardian involvement and clear consent procedures.
- Verify the organizer outside TikTok: official website, company registration, real portfolio, independent mentions, and an official email domain.
- Use a safe submission approach: watermark videos (name/date), avoid sending full ID scans, and share only minimal info until legitimacy is confirmed.
- Ask for a formal casting brief: role description, dates, location, payment terms, privacy policy, data retention, and who processes the data.
- If age verification is required, offer safer alternatives (age declaration, partial redaction of ID, or in-person verification later).
- Keep accounts secured (strong passwords, 2FA) and limit what personal data is publicly visible on profiles.

TikTok Threat

Fake “Contest / Talent Selection” with data & face capture



What to do if it happens?

- Stop communication and do not provide additional videos or documents.
- Save evidence: screenshots of the TikTok, profile, messages, form links, and what you submitted.
- If you sent ID data, monitor for identity misuse (unexpected loan/subscription attempts, strange calls/messages) and tighten security on email/social accounts.
- Report the account and content on TikTok and warn peers if the scam is circulating in your community.
- If the scam escalates to threats/blackmail, involve a trusted adult immediately and report to Romanian authorities; keep all evidence.
- For cyber incidents or suspicious data misuse, report to DNSC/PNRISC and seek guidance.



Severity

- High severity, because it can combine personal data exposure with face/voice capture, enabling impersonation, deepfake misuse, targeted fraud, and potentially coercion or reputational harm.



Key Sources

- TikTok. (n.d.). How to report a problem / report an account. <https://support.tiktok.com/>
- TikTok. (n.d.). Privacy and safety for teens. <https://support.tiktok.com/>
- DNSC. (n.d.). Contact / support & reporting. <https://www.dnsc.ro/contact>
- DNSC. (n.d.). National Cybersecurity Incident Reporting Platform (PNRISC). <https://pnrisc.dnsc.ro/>
- SigurantaOnline.ro. (n.d.). What to do in case of online fraud. <https://sigurantaonline.ro/ce-fac-in-caz-de-frauda/>

Email Threat

Fake Delivery - “customs fee” emails with QR payment links



Main Platform

Email



Short Description

Emails mimic courier/delivery notifications and claim a small outstanding fee, often with a QR code or short link. Victims are directed to a fake payment page that captures card data or triggers subscription fraud.



Typical Youth Scenario

A student or young worker regularly orders online (clothes, electronics, cosmetics) and receives an email that looks like a courier notification. The message says there is a small “customs/handling/redirect” fee and includes a QR code or a short link for fast payment. Because the amount is small and the email feels urgent (“delivery will be returned”), the victim scans the QR code on their phone, enters card details on a convincing payment page, and later discovers unauthorized charges or a recurring subscription.



How does it work?

Scammers send bulk emails that imitate common courier/delivery notifications in Romanian.

The email claims a small outstanding fee (customs/handling/address confirmation) and threatens delay or return of the parcel.

A QR code or shortened link directs the victim to a fake payment page designed for mobile.

The page captures card details and sometimes asks for OTP/3D Secure confirmation.

Victims either get direct card theft (unauthorized transactions) or are enrolled in hidden subscription fraud.

Attackers may reuse the victim’s data for future phishing and targeted scams.

Email Threat

Fake Delivery - “customs fee” emails with QR payment links



Red Flags

- The sender address/domain doesn't match the official courier/company domain (look closely for misspellings).
- Generic greeting and vague parcel details (no real tracking number, no accurate order reference).
- Urgent pressure: “pay today,” “last warning,” “parcel returned,” “delivery failed.”
- The payment is requested via QR/short link rather than through the official courier tracking page/app.
- The link leads to a suspicious domain that doesn't look like a courier or bank payment gateway.
- The message contains language errors, inconsistent branding, or low-quality logos.
- The fee amount is unusually small and designed to feel “safe to pay quickly.”



Prevention Tips

- Never pay delivery/customs fees through QR codes or links received by email—open the courier site/app directly and check your tracking status there.
- Verify sender domain and compare it with the official courier website; treat slight misspellings as a strong warning sign.
- Check for a legitimate tracking number and confirm parcel details via your order platform or official tracking page.
- Avoid scanning QR codes from emails; if you must, inspect the URL before opening and do not proceed if the domain looks unfamiliar.
- Use virtual cards or one-time cards where available for online payments and enable bank alerts for every transaction.
- Keep your browser and phone updated and use spam/phishing filters; report suspicious emails as phishing in your email client.

Email Threat

Fake Delivery - “customs fee” emails with QR payment links



What to do if it happens?

- Stop immediately and do not complete additional steps or payments.
- Save evidence: the email (full headers if possible), screenshots of the QR/link, the payment page, and any transaction confirmations.
- Contact your bank urgently to block the card, dispute charges, and request chargeback where applicable; monitor your account for recurring payments.
- If you entered login credentials anywhere, change passwords immediately and enable 2FA.
- Report the phishing email in your email client and inform the courier company if their brand is being impersonated.
- Report the incident to DNSC/PNRISC and file a police complaint if there is financial loss, using all payment and recipient details.



Severity

- High severity, because a “small fee” lure can quickly lead to card data theft, repeated subscription charges, and broader identity/account compromise.



Key Sources

- Google. (n.d.). Avoid and report phishing emails. <https://support.google.com/mail/answer/8253>
- Microsoft. (n.d.). Protect yourself from phishing. <https://support.microsoft.com/>
- DNSC. (n.d.). Contact / support & reporting. <https://www.dnsc.ro/contact>
- DNSC. (n.d.). National Cybersecurity Incident Reporting Platform (PNRISC). <https://pnrisc.dnsc.ro/>
- SigurantaOnline.ro. (n.d.). What to do in case of online fraud. <https://sigurantaonline.ro/ce-fac-in-caz-de-frauda/>

Conclusions

Romania's youth online safety context is shaped by near-universal, daily internet use among teenagers, which makes TikTok, Instagram, YouTube and messaging (Messenger/WhatsApp) central to how young people socialise, follow trends, and access opportunities. This high-reach, consumption-heavy ecosystem creates fast pathways for risk: harmful content, viral misinformation, risky challenges, and scam funnels can spread quickly through feeds, DMs, link-in-bio pages, and redirects to Telegram/WhatsApp.

A key conclusion is that the main vulnerabilities are not only technical, but strongly behavioural and social. Early entry into social media, very high screen time and peer pressure dynamics increase the likelihood of impulsive clicking/sharing, oversharing personal data, and reacting under urgency—conditions that scammers and manipulators actively exploit. In parallel, cyberbullying and shame-based harassment are amplified by school-linked group dynamics, screenshot culture and “confessions/exposure” pages, which can escalate rapidly and cause significant emotional harm.

Fraud and impersonation risks are particularly salient because they exploit speed and trust: hacked-account money requests, fake giveaways, Marketplace/courier payment links, and phishing disguised as tickets/jobs/scholarships often move youth from TikTok/Instagram to Telegram/WhatsApp and then to cloned forms or fake payment pages. In short-video environments, where emotionally charged content is rewarded and verification is rare, misinformation and influence tactics can also have a disproportionate impact.

Finally, while Romania has clear support and reporting channels (DNSC/PNRISC, Telefonul Copilului 116 111, police reporting), their effectiveness depends on awareness and practical usability for youth and families.

Conclusions

The most relevant response in this national context is therefore a combined approach: practical digital literacy (recognising scam patterns and misinformation cues), account protection habits (2FA, strong passwords, session checks), rapid-response guidance (what to do in the first minutes/hours), and a stronger culture of reporting and support that reduces stigma—especially in harassment, sextortion, and fraud cases.

Resources

- Direcția Națională de Securitate Cibernetică. <https://www.dnsc.ro/contact>
- Direcția Națională de Securitate Cibernetică. National Cybersecurity Incident Reporting Platform (PNRISC). <https://pnrisc.dnsc.ro/>
- Save the Children Romania. (2025, March 28). Study: Almost half of children spend over 6 hours/day in the digital environment. Agerpres. <https://agerpres.ro/english/2025/03/28/save-the-children-study-almost-half-of-children-spend-over-6-hours-day-in-the-digital-environment--1435334>
- Pont Group. (2025, February 24). Findings of the study “The relationship with information and media consumption habits of children and young people in Romania”. <https://en.pontgroup.org/2025/02/24/findings-of-the-study-the-relationship-with-information-and-media-consumption-habits-of-children-and-young-people-in-romania/>
- EU Kids Online. (n.d.). Romania: Country profile. London School of Economics and Political Science. <https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/participating-countries/romania>
- Asociația Telefonul Copilului. (n.d.). Telefonul Copilului – 116111 (Home). <https://telefonulcopilului.ro/>
- Asociația Telefonul Copilului. (n.d.). #BeCyberSafe (Cyberbullying prevention campaign). <https://telefonulcopilului.ro/proiecte/becybersafe/>



ESCAP(E+)

**Istanbul University-
Cerrahpasa IUC**

DESK RESEARCH



Overview

In Türkiye, internet use among children and adolescents is already highly embedded in everyday life. According to TurkStat's 2024 child statistics, 91.3% of children aged 6–15 use the internet and 66.1% use social media; among 11–15-year-olds, internet use reaches 94.7%. Social media is also one of the most common purposes of internet use among regular internet-using children (72.6%). These patterns make social media and e-mail central entry points for online risk, not peripheral spaces.

For Turkish youth, the most relevant cyber risks are not limited to highly technical attacks. Instead, the most common threats are trust-based and behaviour-based: phishing links, fake giveaways, fraudulent shopping or payment requests, impersonation, account takeover, identity theft, and misleading content designed to manipulate attention, beliefs or actions. These risks spread especially well on platforms that combine visual content, direct messaging, comments, sponsored posts and rapid reposting.

The national context also suggests several vulnerability factors. Young users often access the internet primarily through smartphones, interact with influencer or peer-led content, and move quickly between platform content and external links. At the same time, oversharing of personal information, weak password practices, re-use of credentials, low verification habits and the persuasive design of algorithmic feeds can increase exposure to scams and misleading content.

Türkiye has several support and reporting channels that are relevant for youth workers and young people. Technical incidents and harmful cyber threats can be reported to USOM (the national cyber incident response authority). Criminal victimisation, fraud and account misuse can also be escalated to the Cybercrime Department / local cybercrime units of the Turkish National Police. For guidance, prevention and awareness, the Safe Internet ecosystem linked to BTK/GüvenliWeb and the Internet Help Center provides practical support materials.

Overview

Youth Digital Behaviour

In Türkiye, digital connectivity is deeply embedded in young people's everyday lives. According to TurkStat's 2024 child ICT data, 91.3% of children aged 6–15 use the internet regularly and 66.1% use social media regularly. Among regular child internet users, the most common activities are watching videos (83.9%), doing homework or online learning (75.0%), playing or downloading games (72.7%), using social media (72.6%), and messaging (65.2%). Sending and receiving emails is far less common among children (13.2%), suggesting that social platforms and messaging apps dominate daily interaction, while email is used more selectively for school-related communication, registrations, and account recovery.

Among 16–24-year-olds, the pattern becomes even more communication-centred. TurkStat's 2024 youth data shows that the most common internet uses in this age group are texting (98.5%), voice or video calls (95.7%), and social media use (95.3%). Screen exposure is also substantial: among 11–15-year-olds who use smartphones regularly, 15.1% spend six hours or more online on weekends. For this reason, Facebook, Instagram, and TikTok should be understood not as occasional tools but as everyday environments where communication, entertainment, peer influence, and exposure to online risk take place continuously.

Key Risk Factors

One major risk factor in Türkiye is the normalisation of fast, high-frequency clicking, sharing, and reacting behaviours on social platforms. Official Turkish digital safety guidance identifies phishing and social engineering as core threats and warns users not to trust suspicious links, prize or giveaway messages, fast-money offers, threats, fear-based content, or manipulative comments and direct messages. This is especially relevant on Instagram, TikTok, and Facebook, where malicious actors can spread scams through stories, advertisements, fake profiles, comment sections, and private messages. The same manipulation logic also appears in email through fake bank notices, cargo messages, government-style alerts, and account verification requests.

Overview

A second major risk factor is identity theft and account misuse. Turkish guidance on digital identity theft stresses that personal data such as national ID numbers, passwords, addresses, mothers' maiden names, and bank or card details can be stolen through phishing and social engineering, then used for fraudulent financial or administrative actions. A third factor is misinformation and information disorder. SİBERAY notes that social media's weak control mechanisms make it easy for false claims, fake screenshots, panic-inducing posts, and misleading narratives to spread quickly before users verify the original source.

Support and Reporting Channels

In Türkiye, support and reporting should follow a layered approach. First, harmful posts, fake accounts, impersonation attempts, and scam messages seen on Facebook, Instagram, or TikTok should be reported through the platform's own in-app reporting tools so that content removal or account action can begin quickly. At national level, BTK's İhbarWeb and the e-Devlet "İnternet İhbar Başvurusu" service are official routes for reporting illegal online content. In addition, the İnternet Yardım Merkezi provides guidance and practical support for users experiencing online safety problems.

When the issue involves phishing links, malicious websites, identity theft attempts, or broader information-security threats, reports can be submitted to USOM, which operates on a 24/7 basis and provides an official notification form. When a case involves fraud, coercion, extortion, account takeover, or another criminal offence, young people and families can use the Turkish National Police Cybercrime Department's reporting channels or contact the police/112 in urgent cases. Where personal data has been unlawfully processed or exposed, the data subject must first apply to the relevant data controller and may then submit a complaint to the Personal Data Protection Authority (KVKK), including through its complaint module. For preventive support and awareness-raising, GüvenliWeb and SİBERAY also provide public guidance on phishing, social engineering, misinformation, privacy, and safer digital behaviour.

Facebook Threat

Fake Pages, Marketplace Scams, and Fraudulent Links on Facebook



Main Platform

Facebook



Short Description

Threats often appear through fake pages, fraudulent group posts, scam marketplace offers, and malicious links shared in comments or private messages. The goal is usually to steal money, credentials, or personal information.



Typical Youth Scenario

A young person in Türkiye sees a very cheap phone, ticket, or gaming product in a Facebook group or marketplace post. After sending a deposit or entering data through a fake payment page, the item never arrives and personal or financial data may be exposed.



How does it work?

1. The attacker creates a fake profile, page, or listing.
2. An attractive product or urgent message is posted.
3. The victim is pushed to private chat or an external link.
4. The victim pays or shares personal/payment details.
5. The attacker disappears or reuses the data.



Red Flags

Unrealistically low prices;
New or empty seller profiles;
Requests to leave the platform;
Pressure to send a deposit quickly;
Suspicious payment or login links.



Prevention Tips

Verify seller identity and account history;
Avoid advance payments to unknown people;
Never share card or identity details through chat;
Check suspicious offers through official channels;
Use strong passwords and two-factor authentication.

Facebook Threat

Fake Pages, Marketplace Scams, and Fraudulent Links on Facebook



What to do if it happens?

Stop communication immediately.
Contact the bank or payment provider if money was sent.
Change passwords if login details were shared.
Report the profile, page, or listing on Facebook.
Save screenshots and report the incident through national cybercrime channels.



Severity

4/5 - High, because it may lead to both financial loss and misuse of personal data.



Key Sources

GüvenliWeb - online fraud guidance
GüvenliWeb - identity theft guidance
USOM official reporting route
EGM Cybercrime and BTK complaint channels

Instagram Threat

Impersonation, DM Phishing, and Account Hijacking on Instagram



Main Platform

Instagram



Short Description

Cyber threats often appear through fake profiles, compromised accounts, giveaway scams, and direct messages designed to steal credentials or personal information. These attacks rely on trust, curiosity, or social pressure.



Typical Youth Scenario

A teenager in Türkiye gets a DM saying “Is this you in this photo?” or “You won a gift box.” After entering login details through the shared link, the user loses access and the attacker starts messaging followers from the stolen profile.



How does it work?

1. The attacker uses a fake or stolen account.
2. A DM, comment, or story reply creates curiosity or urgency.
3. The victim clicks a malicious link.
4. The victim enters credentials on a fake page.
5. The attacker hijacks the account and targets others.



Red Flags

“You won” messages
Requests for login credentials or verification codes
Unusual messages from a friend
Shortened or non-official links
Fake profiles imitating brands or influencers



Prevention Tips

Verify unusual messages through another channel.
Enable two-factor authentication.
Avoid logging in through links sent in DMs.
Review privacy settings regularly.
Report fake or suspicious accounts immediately

Instagram Threat

Impersonation, DM Phishing, and Account Hijacking on Instagram



What to do if it happens?

Change the Instagram password immediately.
Secure the linked e-mail account.
Warn followers not to trust recent messages.
Report impersonation or hijacking through Instagram.
Keep screenshots and use national reporting channels when needed.



Severity

4/5 - High, because it can expose personal messages, images, contact networks, and identity-related information.



Key Sources

TÜİK - Statistics on Children 2024
TÜİK - Youth Statistics 2024
GüvenliWeb - identity theft and online scam guidance
USOM and EGM Cybercrime reporting channels

TikTok Threat

Viral Misinformation, Scam Redirects, and Manipulative Content on TikTok



Main Platform

TikTok



Short Description

Cyber-related risks often spread through viral videos, misleading claims, fake opportunities, and malicious redirects placed in bios, comments, or private messages. The fast circulation of content increases the risk of misinformation and unsafe clicking behaviour.



Typical Youth Scenario

A young user in Türkiye watches a trending video claiming that a scholarship, state support payment, or reward can be obtained through a link in the bio. The user clicks through and submits personal data on a fake page.



How does it work?

1. The attacker shares emotional or sensational content.
2. The video encourages users to act immediately.
3. The victim follows a link in bios, comments, or messages.
4. The victim enters credentials, personal data, or payment details.
5. The attacker harvests data or continues spreading the scam.



Red Flags

Viral claims without an official source
 "Act now" or fear-based messaging
 Instructions to use a link in bio for sensitive actions
 Edited screenshots or clips with unclear origin
 Requests for passwords, ID details, or payment information



Prevention Tips

Verify important claims through official institutions.
 Do not trust information only because it is trending.
 Be cautious with links in bios, comments, and DMs.
 Adjust privacy settings to reduce unwanted contact.
 Pause before reacting to emotional or urgent content.

TikTok Threat

Viral Misinformation, Scam Redirects, and Manipulative Content on TikTok



What to do if it happens?

Stop sharing the content immediately.
Delete any repost if the content is false.
Take screenshots for evidence.
Report the video or account within TikTok.
Change passwords if any credentials were submitted and report serious cases.



Severity

4/5 - High, because misinformation can drive unsafe behaviour and scam redirects may result in data theft.



Key Sources

TÜİK - Statistics on Children 2024
TÜİK - Youth Statistics 2024
SİBERAY - information disorder guidance
USOM, EGM Cybercrime, BTK, and KVKK resources

Email Threat

Credential Phishing and Account Takeover via E-mail



Main Platform

E-mail



Short Description

Fraudulent e-mails imitate trusted institutions such as banks, universities, cargo companies, scholarship providers, or public bodies. The aim is to make young users click fake links, enter credentials, share personal data, or download malicious attachments.



Typical Youth Scenario

A student in Türkiye receives an e-mail claiming that a school account, scholarship application, or package delivery needs urgent verification. The message looks legitimate, so the student enters login details on a fake page and later loses access to the mailbox or linked accounts.



How does it work?

1. A fake e-mail is sent.
2. It creates urgency, fear, or curiosity.
3. The victim clicks a malicious link or opens an attachment.
4. The victim reaches a fake login page or installs malware.
5. Credentials or data are stolen and reused.



Red Flags

Urgent verification requests
Suspicious sender addresses or domains
Generic greetings
Unexpected prize, refund, or delivery notices
Requests for passwords, OTP codes, or banking details



Prevention Tips

Do not click suspicious links or attachments.
Check the sender address carefully.
Use official websites instead of message links.
Enable strong passwords and two-factor authentication.
Never share passwords, OTP codes, or card information by e-mail.

Email Threat

Credential Phishing and Account Takeover via E-mail



What to do if it happens?

Stop interacting with the e-mail.
Change the affected password.
Reset two-factor authentication if needed.
Scan the device for malware.
Report the incident to the provider and Turkish cybercrime channels.



Severity

5/5 - Very high, because compromise can lead to identity theft, financial fraud, and access to multiple linked services.



Key Sources

TÜİK - Statistics on Children 2024; Youth Statistics 2024
GüvenliWeb - phishing and online fraud guidance
USOM, BTK, EGM Cybercrime, and KVKK reporting resources

Conclusions

These threats are the most relevant in Türkiye because they align closely with how young people actually use digital environments: frequently, visually, socially and mostly through mobile devices. The strongest risks are therefore not abstract cyber attacks but everyday manipulations that use trust, urgency, identity and platform familiarity.

For youth workers, the main implication is that cybersecurity education should be practical, scenario-based and platform-specific. Young people need to recognise phishing beyond e-mail, understand how personal data fuels impersonation, and develop habits for checking sources before sharing or acting.

The findings support the ESCAP(E+) outputs in several concrete ways. In the project framework and training guidance, emphasis should be placed on verification routines, privacy settings, two-factor authentication, account recovery, safe reactions to suspicious messages, and the use of local reporting routes. For the VR escape game, strong scenarios would include a fake giveaway, a cloned Instagram profile, a direct message asking for a code or payment, a false 'official' alert, or a TikTok-style viral misinformation chain. For infographics and animated awareness materials, the content should be short, visual, youth-friendly and rooted in real platform behaviours rather than generic cyber terminology.

Resources

- TurkStat (2025). Türkiye'deki Çocuklar 2024 İstatistiklere Bakış / Statistics on Child 2024. https://www.tuik.gov.tr/media/announcements/Turkiye_Cocuk_2024TR.pdf
- Emniyet Genel Müdürlüğü (EGM). Siber Suçlarla Mücadele Daire Başkanlığı. <https://www.egm.gov.tr/siber>
- Emniyet Genel Müdürlüğü (EGM). Sosyal Medya Dolandırıcılığı. <https://www.egm.gov.tr/sosyal-medya-dolandiriciligi>
- Emniyet Genel Müdürlüğü (EGM). Siber Suçlarla Mücadele – Sıkça Sorulan Sorular. <https://www.egm.gov.tr/siber/sikca-sorulan-sorular>
- Ulusal Siber Olaylara Müdahale Merkezi (USOM). Official website and contact/reporting channels. <https://www.usom.gov.tr/>
- GüvenliWeb. İnternet Dolandırıcılarına Geçit Vermeyin! <https://www.guvenliweb.org.tr/haber-detay/internet-dolandiricilarina-gecit-vermeyin>
- GüvenliWeb. Sosyal Mühendislik Riskleri. <https://www.guvenliweb.org.tr/index-orj.php/blog-detay/sosyal-muhendislik-riskleri>
- GüvenliWeb. Çocuklarda Dijital Mahremiyet Bilinci. <https://www.guvenliweb.org.tr/blog-detay/cocuklarda-dijital-mahremiyet-bilinci>
- GüvenliWeb. İnternet ve Bilgi Güvenliği. <https://www.guvenliweb.org.tr/blog/internet-ve-bilgi-guvenligi>
- GüvenliWeb. Dezenformasyonun Yayılma Yolları ve Önlenmesi. <https://www.guvenliweb.org.tr/blog-detay/dezenformasyonun-yayilma-yollari-ve-onlenmesi>
- GüvenliWeb. 7 Adımda Dezenformasyonu Önlemenin Yolları. <https://www.guvenliweb.org.tr/blog-detay/7-adimda-dezenformasyonu-onlemenin-yollari>
- GüvenliWeb. Sosyal Medya Algoritmaları ve Çocuklar Üzerindeki Etkisi. <https://www.guvenliweb.org.tr/blog-detay/sosyal-medya-algoritmaları-ve-cocuklar-uzerindeki-etkisi>
- EU Kids Online Turkey (2015 summary report). The changes in safer internet use of children in Turkey. https://eukidsonline.metu.edu.tr/tr/system/files/raporlar/euko_turkey2015_summaryreport.pdf



ESCAP(E+)

Estonia

DESK RESEARCH



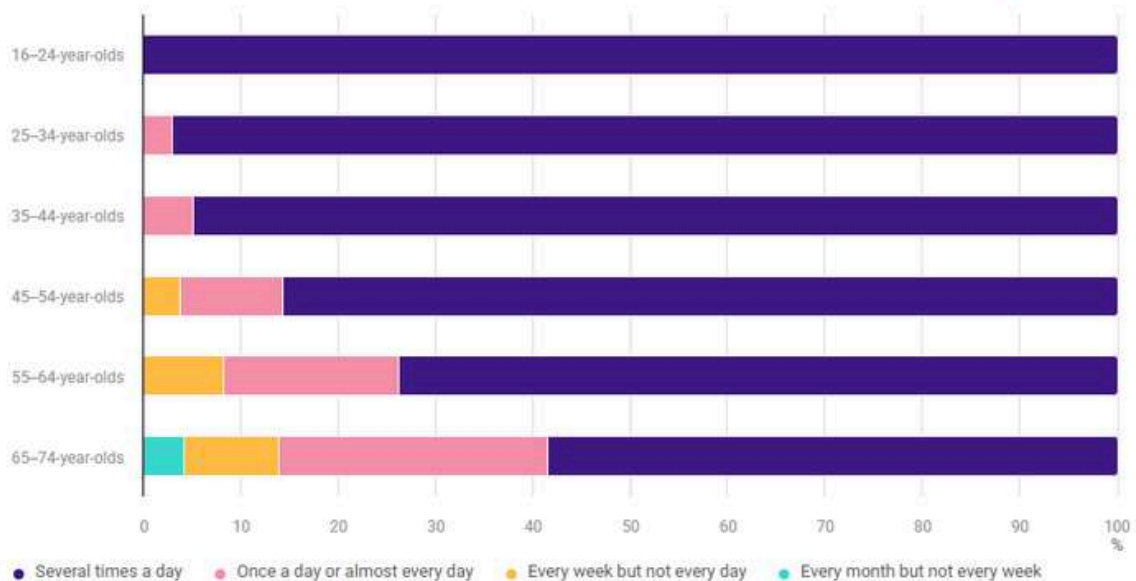
Overview

Estonia is widely recognised as one of the most digitally advanced societies in Europe. Over the past two decades, extensive national investment in digital infrastructure, e-government services and digital education initiatives has shaped a highly connected environment in which young people grow up. As a result, digital technologies are deeply embedded in the everyday lives, learning practices and social interactions of Estonian youth.

Access to digital technology among young people in Estonia is almost universal. According to “Statistics Estonia”, 93.2% of households in Estonia have an internet connection at home and usage is particularly high among younger age groups as depicted in the diagram below:

Frequency of internet use by age group, 2023

Source: Statistics Estonia

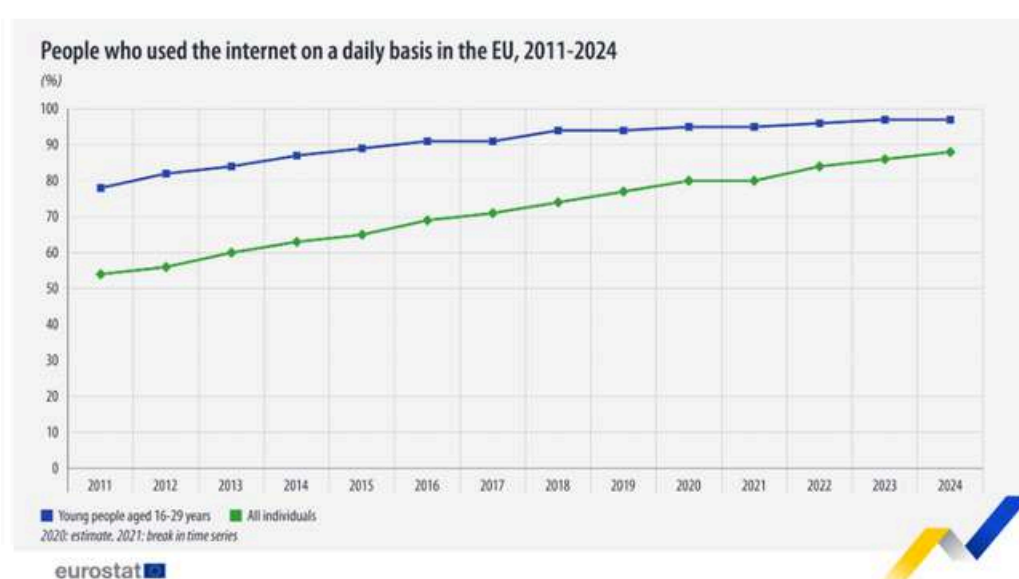


Overview

Sigrid Saagpakk, analyst at Statistics Estonia, explained that the internet and online services play an increasingly bigger role in people's lives: "By age group, the share of internet users is the highest among young people, as almost 100% of them use the internet. Internet use is the most frequent among 16–24-year-olds, with 96% of them using the internet several times a day."

Digital technology is strongly integrated into Estonia's education system and youth development policies. Schools often encourage the use of digital tools in learning environments rather than restricting them. National initiatives continue to promote digital literacy, coding skills and emerging technologies such as artificial intelligence, to prepare students for participation in a digital economy and knowledge society.

These trends align with broader European patterns. Based on Eurostat's data, internet use among young people across the European Union is extremely high: 97% of EU citizens aged 16–29 reported using it daily in 2024, compared to 88% of the general population, as depicted in the diagramme below:



Overview

In all EU countries, young people were much more likely to participate in social network activities than the total population. Creating a user profile and posting messages or related activities was a widespread practice for 88% of 16 to 29-year-olds compared with 65% of the total population. However, Estonia often performs above the EU average in digital competence indicators. According to the European Commission's Digital Decade Report 2024, 62.6% of Estonia's population possesses at least basic digital skills, exceeding the EU average of 55.6%. Estonia also has a higher proportion of ICT specialists in the workforce than the EU average, reflecting the country's long-standing policy focus on digital innovation and digital education.

Key Risk Factors

Despite the many opportunities provided by digital technologies, young people in Estonia face several online safety risks. Research from the EU Kids Online project indicates that Estonian children are exposed to a range of potentially harmful online experiences, including cyberbullying, contact with strangers and exposure to harmful or inappropriate content. According to the findings of the aforementioned project, 97% of Estonian children aged 9–17 access the internet every day using at least one device. Online communication is a major aspect of youth social life: 46% of children reported having contact online with someone they had not previously met face-to-face and approximately one third of these children had subsequently met that person offline.

Studies show that a significant proportion of Estonian youth have encountered online hate speech, violent content or misleading information, reflecting broader trends observed across Europe. High levels of internet use, particularly through smartphones and social media platforms, increase the likelihood of encountering these risks. In addition, young people may face challenges related to privacy, such as sharing personal information online or being targeted by scams or manipulation.

Overview

Key National Indicators

Other EU-level analyses also highlight challenges related to online safety and digital well-being. Eurostat data show that 49% of young Europeans aged 16–29 reported encountering hostile or abusive online messages in 2023. Estonia recorded one of the highest reported exposure rates at 69%, reflecting both the high level of online engagement and the increasing prevalence of harmful digital content.

Support and Reporting Channels

Estonia has several official support and reporting channels that young people, parents and educators can use when facing online risks such as cyberbullying, grooming or exposure to harmful content. One of the most important services is the Estonian Child Helpline (Lasteabi), which operates a free 24-hour helpline (116 111) providing counselling and advice for children, parents and professionals regarding issues such as cyberbullying, online harassment and harmful online content. The service can also be contacted via online chat or email and allows users to remain anonymous if needed.

The Estonian Hotline Vihjeliin enables users to report illegal online material, especially content regarding children sexual abuse, so that it can be assessed and forwarded to law enforcement authorities for removal. These services operate as part of the wider Estonian Safer Internet Centre initiative, which promotes awareness, education and support mechanisms to improve digital safety among children and young people.

Facebook Threat

Misinformation & Disinformation Campaigns



Main Platform

Facebook



Short Description

Young people encounter and amplify false or misleading content – from health hoaxes to politically motivated narratives. Facebook's algorithm prioritises engagement over accuracy and Estonia's proximity to Russia makes it a frontline target for coordinated information operations aimed at its Russian-speaking minority and wider population.



Typical Youth Scenario

A 17-year-old student in Tallinn sees a Facebook post shared by a classmate claiming that a new EU regulation will ban encrypted messaging apps. The post includes a professional-looking graphic and links to a fake news site. Without checking the source, the student shares the post to their own feed and a school group chat, spreading the false claim to dozens of peers. Several friends become alarmed and begin sharing it further, generating anxiety and distrust toward EU institutions – exactly the reaction the original disinformation campaign intended.



How does it work?

1. A state-sponsored actor or organised group creates a fake news article or manipulated image designed to provoke an emotional reaction – outrage, fear, or distrust – around a politically or socially sensitive topic.
2. The content is seeded across Facebook through fake accounts, bot networks, or compromised pages that appear to be legitimate local news outlets or community groups.
3. Facebook's engagement-driven algorithm detects high interaction (angry reactions, comments, shares) and amplifies the content into the feeds of more users, including young people who follow related topics or groups.
4. Young users, who tend to consume news primarily through social media and may lack source-verification habits, share the content with their own networks – often adding personal commentary that lends it further credibility among peers.
5. By the time fact-checkers flag the content, it has already reached thousands of users. The emotional impression persists even after corrections are issued, as studies show that retractions rarely reach the same audience as the original false claim.

Facebook Threat

Misinformation & Disinformation Campaigns



Red Flags

The source is an unfamiliar website with no clear editorial team, contact details, or publication history. The headline uses extreme or emotionally charged language designed to provoke immediate outrage or panic. The content has no named author or quotes unnamed "experts" and "officials" without specifics. The post urges you to "share before they delete this" or implies censorship to create urgency. Images or statistics are presented without context, dates, or verifiable sources. The story cannot be found on any established news outlet – only on obscure pages or hyper-partisan groups. The Facebook page sharing it was recently created, has an inconsistent posting history, or posts exclusively on one divisive topic.



Prevention Tips

Always check whether the story is reported by at least two established, independent news sources before sharing. Use fact-checking tools such as EUvsDisinfo.eu, Propastop.org (Estonia's own disinfo tracker), or AFP Fact Check. Examine the source – click through to the website, check the "About" page, and look at the domain name for irregularities. Pause before sharing emotionally charged content; disinformation is designed to bypass critical thinking by triggering strong feelings. Adjust Facebook feed preferences to prioritise trusted news sources and reduce algorithmic recommendations from unknown pages. Discuss media literacy with peers – young people are more likely to listen to friends than to institutional warnings. Report suspected disinformation directly to Facebook using the "Find support or report post" option.

Facebook Threat

Misinformation & Disinformation Campaigns



What to do if it happens?

Stop sharing the content immediately and delete your post if you have already shared it. Inform friends or group members who may have seen it that the content is unverified or false and share a link to a credible fact-check if one exists. Report the post and the page to Facebook as misinformation using the platform's built-in reporting tools. If the disinformation targets a specific community or relates to elections, report it to Estonia's CERT-EE (cert@cert.ee) or the Police and Border Guard Board. Reflect on what made the content convincing – this builds personal resilience against future disinformation attempts. If the content was part of a coordinated campaign targeting Estonian or EU interests, flag it to [Propastop.org](https://propastop.org) or [EUvsDisinfo.eu](https://euvsdisinfo.eu) for documentation and public awareness.



Severity

Likelihood 4/5 – This type of threat is widespread and persistent across the EU. Estonia is a particularly high-exposure country due to its border with Russia, large Russian-speaking population, and highly digitalised society. Facebook remains one of the primary vectors for cross-border disinformation campaigns, and young people are disproportionately reliant on social media as a news source, making them both targets and unwitting amplifiers. The European Commission's 2024 report on the Digital Services Act flagged systemic misinformation risks on large platforms as an ongoing concern.



Key Sources

- EUvsDisinfo.eu – EU East StratCom Task Force disinformation database: <https://euvsdisinfo.eu>
- Propastop.org – Estonian volunteer-run disinformation monitoring: <https://www.propastop.org/en/>
- RIA Cyber Security in Estonia 2026 report: <https://www.ria.ee/en/cyber-security-estonia-2026>
- European Commission Digital Services Act enforcement updates: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- Molly Rose Foundation research on algorithmic amplification of harmful content: <https://mollyrosefoundation.org>
- F-Secure Scam Intelligence & Impacts Report 2025: <https://www.f-secure.com/us-en/partners/insights/scam-intelligence-and-impacts-report-2025>

Instagram Threat

Sextortion & Sexual Blackmail



Main Platform

Instagram



Short Description

Criminals posing as romantic interests contact teenagers via DMs, solicit intimate images and then threaten to share them unless the victim pays or provides more content. The FBI has reported a 1,000% increase in sextortion incidents, with Instagram identified as a primary platform. Two families have sued Meta alleging the platform ignored these dangers, with one boy joining Instagram and dying by suicide within two days.



Typical Youth Scenario

A 16-year-old boy in Tartu receives a follow request on Instagram from an attractive girl who appears to be a similar age. Her profile looks genuine – selfies, tagged friends, casual stories. After a few days of friendly messaging, the conversation turns flirtatious and she suggests they exchange private photos. He sends an intimate image. Within minutes, the tone changes completely. The account sends a screenshot of his photo alongside his follower list and demands €200 via cryptocurrency within one hour, threatening to send the image to his classmates, parents, and teachers. Panicked and ashamed, he pays – but a second demand follows immediately. He feels unable to tell anyone and withdraws from school and social life over the following weeks.



How does it work?

Organised criminal networks – frequently operating from West Africa or Southeast Asia – create convincing fake Instagram profiles using stolen photos of attractive young people. They populate the accounts with posts, stories, and followers to appear authentic.

The scammer sends follow requests or DMs to a large number of teenagers, often identified through public-school accounts, hashtags, location tags, or follower lists of youth-oriented pages. Initial messages are casual and friendly to establish rapport.

Over hours or days, the conversation is steered toward romantic or sexual topics. The scammer may send fake intimate images first to create a sense of reciprocity and lower the target's guard, then encourages the victim to share their own photos or video.

Instagram Threat

Sextortion & Sexual Blackmail

- Once intimate material is received, the scammer immediately reveals their true intent. They screenshot the victim's follower list or friend connections and threaten to distribute the images to family, friends, and schoolmates unless the victim sends money – typically via gift cards, cryptocurrency, or mobile payment apps.
- Payment rarely ends the extortion. Scammers escalate demands, request additional content, or sell the material to other criminal networks. Victims – overwhelmed by shame, fear, and isolation – often suffer severe psychological harm. In the most tragic cases, this has led to self-harm and suicide among teenage boys in particular.



Red Flags

A stranger with an attractive profile sends a follow request or DM out of nowhere, especially if you have no mutual connections. The conversation moves unusually fast from casual chat to flirtatious or sexual topics within hours or days. They insist on moving the conversation to a different platform – such as Snapchat, WhatsApp, or a video chat service – where they claim it will be "more private." They send intimate images of themselves early in the conversation without being asked, creating pressure to reciprocate. Their profile is relatively new, has few posts compared to followers, or features photos that look overly polished or inconsistent. They avoid video calls or make excuses when asked to speak live – because their appearance does not match their profile. They express unusually intense emotional attachment very quickly, using phrases like "I've never felt this way about anyone" to build false intimacy. Any request for intimate photos or videos, regardless of how comfortable the conversation feels, should be treated as a serious warning sign.



Prevention Tips

Never share intimate images or videos with anyone online, regardless of how well you think you know them – once sent, you lose all control over the content. Set your Instagram account to private and do not accept follow requests from people you do not know in real life. Be cautious of new contacts who quickly steer conversations toward romantic or sexual topics.

Instagram Threat

Sextortion & Sexual Blackmail

Disable the ability for strangers to message you directly by adjusting Instagram's message request settings under Privacy controls. If you are under 18, enable Instagram's Teen Account features, which restrict contact from strangers and limit exposure to sensitive content. Talk openly with trusted friends or adults about online relationships – sextortion thrives on silence and isolation. Remember that sharing someone else's intimate images is illegal in Estonia and across the EU, so the person threatening you is the one committing a crime, not you. Use reverse image search (such as Google Images or TinEye) to check whether a new contact's profile photos appear elsewhere online under a different name.



What to do if it happens?

Do not pay the extortionist – payment almost never stops the threats and typically leads to escalating demands. Do not delete the messages, images, or account interactions – save screenshots of everything as evidence, including the scammer's username, profile, and all messages. Stop all communication with the scammer immediately – do not respond to further threats or negotiate. Report the account to Instagram directly using the in-app reporting function, selecting "scam or fraud" and "sexual exploitation" as categories. Contact the Estonian Police and Border Guard Board (report online at politsei.ee or call 112 in an emergency) – sextortion is a criminal offence and law enforcement can act on reports. Reach out to a trusted adult – a parent, teacher, school counsellor, or youth worker. If you are not comfortable speaking to someone you know, contact Estonia's child helpline at 116 111 (free, confidential, 24/7). Report the incident to the National Centre for Missing and Exploited Children's CyberTipline (report.cybertip.org) or the EU's Safer Internet helpline in Estonia via the Lasteabi service. Remember that you are the victim – the shame belongs entirely to the criminal. Thousands of young people across Europe have been targeted by these organised networks, and seeking help is the strongest action you can take. If you are in emotional distress or having thoughts of self-harm, contact Estonia's crisis helpline at 116 123 or the pan-European emotional support line at 116 006.

Instagram Threat

Sextortion & Sexual Blackmail



Severity

Likelihood 5/5 – This is one of the most dangerous and rapidly growing cyber threats targeting young people across the EU. Sextortion attacks are carried out by organised criminal networks at industrial scale, with the FBI, Europol, and Estonia's own Police and Border Guard Board all flagging a sharp rise in cases. Instagram has been specifically identified in multiple lawsuits and law enforcement reports as a primary vector. Boys aged 14–17 are disproportionately targeted, and the psychological consequences – including severe anxiety, social withdrawal, and suicide – make this among the highest-severity threats in the youth cybersecurity landscape. Estonia's digitally connected youth population and high social media usage rates place young Estonians at significant exposure.



Key Sources

Network Contagion Research Institute report on Yahoo Boys and financial sextortion: <https://networkcontagion.us>
NBC News report on Meta sextortion lawsuits (December 2025): <https://www.nbcnews.com/tech/social-media/two-families-sue-meta-teens-deaths-suicide-citing-sex-tortion-scams-rcna248136>
Estonian Police and Border Guard Board online reporting: <https://www.politsei.ee/en>
Estonian child helpline (Lasteabi): <https://www.lasteabi.ee/en>
Better Internet for Kids – Estonian Safer Internet Centre: <https://better-internet-for-kids.europa.eu/en>
Europol Internet Organised Crime Threat Assessment (IOCTA): <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment>

TikTok Threat

Misinformation via Viral Trends



Main Platform

TikTok



Short Description

Short-form video culture encourages rapid sharing of unverified claims – from dangerous health challenges to political falsehoods. TikTok's For You Page algorithm can rapidly amplify misleading content to millions of young users before fact-checkers can respond, making it a significant vector for disinformation across EU member states.



Typical Youth Scenario

A 15-year-old student in Pärnu opens TikTok after school and sees a video with 800,000 views claiming that a common energy drink ingredient causes heart failure in teenagers. The video features dramatic music, a screenshot of what appears to be a medical journal, and a creator speaking with conviction. The student immediately shares it to a class group chat on WhatsApp, warning friends to stop drinking it. Within hours the claim has spread across the school. A parent contacts the school in alarm. When a teacher investigates, the "medical journal" screenshot turns out to be a fabricated image – the study never existed. But the panic has already disrupted the school day, and weeks later some students still believe the claim because they never saw a correction.



How does it work?

A creator posts emotional or alarming content to gain views, influence opinions, or support a wider disinformation campaign. The video receives shares and comments, so TikTok shows it to more users. Young people may then spread it through WhatsApp, Instagram, or school chats.

Viewers share the content across platforms – to WhatsApp groups, Instagram stories, Snapchat, and school forums – amplifying its reach far beyond TikTok itself. Each share adds a layer of social proof, as young people are more likely to trust content forwarded by friends than content from unknown sources. By the time fact-checkers, platform moderators, or trusted adults flag the content, it has already been viewed millions of times and internalised by a significant portion of its audience.

TikTok Threat

Misinformation via Viral Trends



Red Flags

The video makes a dramatic or alarming claim but provides no verifiable source – no named study, no linked article, no credited expert. The creator uses highly emotional language, urgent music, or shock tactics designed to provoke an immediate reaction rather than thoughtful consideration. Screenshots of "evidence" such as news headlines, scientific papers, or official statements appear in the video but are too blurry to read, oddly cropped, or cannot be found through a simple web search. The claim is only circulating on TikTok or other social media platforms and is not reported by any established news outlet or fact-checking organisation. The video encourages viewers to "share before it gets taken down" – a common manipulation tactic that frames potential content moderation as censorship to create urgency.



Prevention Tips

Pause before sharing any content that triggers a strong emotional reaction – misinformation is engineered to bypass critical thinking by exploiting fear, anger, or shock. Check whether the claim is reported by at least two established, independent news sources before believing or sharing it. Use EU-supported fact-checking tools such as EUvsDisinfo.eu, AFP Fact Check, or Full Fact to verify suspicious claims. Look up the original source cited in the video – if no source is given, or the cited study or article does not exist, treat the claim as unverified. Follow trusted accounts on TikTok that specialise in debunking misinformation, such as media literacy organisations or verified journalists. Be especially sceptical of health claims, political statements, and crisis-related content on TikTok – these are the topics most commonly targeted by disinformation campaigns. Discuss what you see online with friends, teachers, or family – talking through suspicious content with others is one of the most effective defences against misinformation. Adjust your TikTok settings to reduce algorithmic recommendations by clearing watch history periodically and using the "Not Interested" feature on sensational content. Learn to distinguish between opinion, satire, and factual reporting – media literacy is a skill that improves with practice and is part of Estonia's national digital education curriculum.

TikTok Threat

Misinformation via Viral Trends



What to do if it happens?

If you have already shared misinformation, delete your post or message and inform the people you shared it with that the content was false. Report the misleading video to TikTok using the in-app reporting function, selecting "misinformation" as the category. If the misinformation appears to be part of a coordinated campaign, report it to EUvsDisinfo.eu or Estonia's Information System Authority (RIA) for documentation. Talk to a teacher, school librarian, or youth worker if you are unsure whether something you saw is true. There is no shame in checking, and building the habit of verification strengthens your long-term resilience against disinformation. If misinformation has caused real distress speak to a trusted adult or contact Estonia's youth support line at 116 111.



Severity

Likelihood 4/5 – This threat is pervasive and affects virtually all young TikTok users across the EU. TikTok is the primary news source for a growing proportion of European teenagers, and its algorithm is structurally designed to prioritise engagement over accuracy. Estonia faces elevated risk due to its position as a target for Russian-language disinformation operations, its highly digitalised youth population, and the speed at which false content can spread in a small, tightly connected society.



Key Sources

EUvsDisinfo.eu – EU East StratCom Task Force disinformation database: <https://euvsdisinfo.eu>

Propastop.org – Estonian volunteer-run disinformation monitoring: <https://www.propastop.org/en>

European Commission – DSA enforcement and TikTok as a VLOP: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

Molly Rose Foundation – research on algorithmic amplification of harmful content to teens: <https://mollyrosefoundation.org>

RIA Cyber Security in Estonia 2026 report: <https://www.ria.ee/en/cyber-security-estonia-2026>

Reuters Institute Digital News Report – youth news consumption trends: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report>

Better Internet for Kids – Estonian Safer Internet Centre and SID 2025 activities: <https://better-internet-for-kids.europa.eu>

Email Threat

Fake Job & Internship Offers



Main Platform

Email



Short Description

Scammers target students with mass emails offering easy money through "secret shopper" roles, remote assistant positions, or paid internships. Victims are tricked into depositing fraudulent cheques, purchasing gift cards, or sharing personal details. University and school email addresses are specifically targeted because students are financially pressured and less security-experienced.



Typical Youth Scenario

A 19-year-old university student in Tallinn receives an email to her institutional address from someone claiming to be a professor at a partner university offering a part-time remote research assistant role paying €400 per week. The email is well-written, references her field of study, and includes a university logo. She replies expressing interest. The sender asks her to complete an onboarding form with her full name, address, date of birth, phone number, and bank details "for payroll setup." She is then sent a €1,500 cheque by courier and instructed to deposit it immediately, keep €400 as her first payment, and use the remainder to purchase digital gift cards for "research participant incentives," sending the codes back by email. Her bank initially shows the funds as available, so she buys the gift cards and sends the codes. Three days later, the cheque bounces, the €1,100 she spent on gift cards is gone, her bank charges an overdraft fee, and the scammer's email address no longer exists. She is left with a financial loss, compromised personal data, and the stress of reporting the incident during exam season.



How does it work?

Scammers collect student email addresses from university websites, directories, LinkedIn, or other online platforms. They send professional-looking messages using university logos, copied names, or compromised accounts to appear credible. Students who respond are asked for personal details, bank information, or help with "payments." In some cases, they are told to deposit a cheque, transfer money, or buy gift cards. Once the scammer receives the money or codes, they disappear.

Email Threat

Fake Job & Internship Offers



Red Flags

- The offer arrives unexpectedly and was not advertised through an official career portal.
- The pay is unusually high for simple or flexible work.
- The sender uses a personal email address instead of an official institutional domain.
- The employer asks for ID details, bank information, or home address before an interview or contract.
- The role involves depositing cheques, transferring money, or buying gift cards.
- The message creates urgency and pressures the student to act quickly.



Prevention Tips

Verify any unsolicited job offer independently before responding – search for the company or organisation on official registers (in Estonia, use the e-Business Register at ariregister.rik.ee), check their website, and call their listed phone number to confirm the role exists. Never provide sensitive personal information – national ID number, bank account details, date of birth, or home address – to an employer you have not met in person or verified through your university's career services. If the offer claims to come from a professor or staff member at your own institution, contact that person directly through official university channels to confirm – do not reply to the email itself. Use your university's official career portal or trusted EU-wide platforms such as EURES (eures.europa.eu) or Erasmus+ Intern to find legitimate opportunities. Be immediately suspicious of any role that involves depositing cheques, forwarding money, or purchasing gift cards – these are hallmarks of fraud, not employment. Discuss unexpected job offers with a trusted adult, university career adviser, or student union representative before taking any action. Enable two-factor authentication on your university email account to reduce the risk of your own address being compromised and used to target fellow students. Remember that legitimate employers in the EU are required to provide a written employment contract before work begins – if no contract is offered, the opportunity is not genuine.

Email Threat

Fake Job & Internship Offers



What to do if it happens?

- Stop communication immediately.
- Save screenshots of emails, payment requests, sender addresses, and transaction records.
- Contact your bank if you shared financial details or made a payment.
- Report the incident to the Estonian Police and Border Guard Board.
- Inform your university IT/security team so they can warn other students.
- If personal identity data was shared, contact the Estonian Information System Authority for guidance.



Severity

Likelihood 4/5 – Fake job and internship scams are highly relevant for students because they exploit financial pressure, trust in academic institutions, and the frequent use of university email. The threat can lead to financial loss, identity theft, and emotional stress.



Key Sources

Estonian Police and Border Guard Board – online fraud reporting: <https://www.politsei.ee>

RIA – Estonian Information System Authority and CERT-EE: <https://www.ria.ee/en>

Estonian e-Business Register (company verification): <https://ariregister.rik.ee/eng>

EURES – EU-wide legitimate job portal: <https://eures.europa.eu>

UC Berkeley Information Security Office – phishing examples archive (university-targeted scams): <https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive>

NYU Information Technology – top cybersecurity scams targeting students: <https://www.nyu.edu/life/information-technology/safe-computing/checklists-guides/cyberthreats/scams-targeting-students.html>

F-Secure Scam Intelligence & Impacts Report 2025: <https://www.f-secure.com/us-en/partners/insights/scam-intelligence-and-impacts-report-2025>

Better Internet for Kids – Safer Internet Day 2025 resources on scams affecting young people: <https://better-internet-for-kids.europa.eu>

Conclusions

Overall it can be said that Estonia's youth digital environment is characterised by widespread access to technology, high levels of digital competence and strong institutional support for digital learning. European Union research consistently positions Estonia among the leading digital societies in Europe. Nevertheless, the extensive use of digital media among young people also highlights the importance of addressing issues related to online safety, cyberbullying, digital well-being and critical digital literacy. Therefore, policymakers and educators increasingly emphasise responsible online behaviour, media literacy and digital resilience as key competencies for young people growing up in Estonia's highly digitalised society.

The European Commission and Eurostat reports also highlight growing concerns about cyberbullying, online harassment and the spread of harmful digital content among adolescents in the European Union. That is why researchers and policymakers emphasise the importance of strengthening digital literacy, critical media skills and online safety education in order to help young people navigate digital environments safely and responsibly.

The findings of this desk research showed that there are many threats to which young people are exposed while using Social Media or even their email. The ESCAP(E+) project aims to develop comprehensive resources for young people, such as interactive digital tools, including a VR Escape Game App, infographics and animated videos, in order to promote their digital inclusion and raise their awareness in terms of cybersecurity and online safety practices among young people.

Resources

- “Estonia: a snapshot of digital skills”, created by Lidija Kralj, updated on the 2nd of August 2024 and accessed on the 11th of March 2026 <https://digital-skills-jobs.europa.eu/en/latest/briefs/estonia-snapshot-digital-skills>
- euronews, article: “Nearly half of EU youngsters exposed to online abuse, new report finds”, by Alessio Dell’Anna, published on 07/11/2024 and accessed on the 11th of March 2026 <https://www.euronews.com/my-europe/2024/11/07/nearly-half-of-eu-youngsters-exposed-to-online-abuse-new-report-finds>
- European Union, Better Internet for Kids, Estonian Safer Internet Center, accessed on the 12th of March 2026 <https://better-internet-for-kids.europa.eu/en/sic/estonia>
- Eurostat, article: “97% of young people in the EU use the internet daily” published on the 15th of July 2025 and accessed on the 11th of March 2026 <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20250715-1>
- London School of Economics and Political Science. (2020). “EU Kids Online: Estonia country findings” accessed on the 11th of March 2026 <https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/participating-countries/estonia>
- Republik of Estonia, Social Insurance Board, “Child Helpline 116111”, accessed on the 12th of March 2026 <https://sotsiaalkindlustusamet.ee/en/child-and-adult-need-help/child-protection-and-family-support/child-helpline-116111>
- Statistics Estonia: “Internet use is increasing in Estonia”, posted on the 14th of September 2023 and accessed on the 11th of March 2026 <https://stat.ee/en/news/information-technology-households-2023>



ESCAP(E+)

Spain

DESK RESEARCH



Overview

National statistics demonstrate that internet use among young people in Spain is extremely widespread. Data from the Spanish National Statistics Institute (INE) indicate that 99.6% of individuals aged 16-24 are regular internet users. Digital tools are commonly used for communication, entertainment, academic purposes, and information access. Social media platforms such as Instagram and TikTok, as well as messaging applications like WhatsApp, play a central role in the daily interactions of adolescents and young adults.

For most Spanish youth, smartphones constitute the main gateway to online environments. Continuous connectivity enables frequent engagement in private messaging, content sharing, and participation in online communities. However, this high level of exposure also increases interaction with unknown contacts, suspicious links, and potentially unsafe digital spaces.

Key Risk Factors

In Spain, high levels of youth digital engagement coexist with persistent gaps in cybersecurity awareness and digital safety competence. Reports and awareness initiatives promoted by the Spanish National Cybersecurity Institute (INCIBE) indicate that many young users underestimate online risks and demonstrate limited knowledge of data protection principles, privacy awareness, and online risk prevention strategies.

The intensive use of social media platforms and private messaging services increases exposure to unfamiliar contacts, external links, and rapidly shared digital content. When combined with rapid smartphone-based responses and reduced critical evaluation of online information, these patterns may weaken cyber resilience and facilitate vulnerability to social engineering techniques, phishing attempts, misinformation, identity theft, and other forms of online fraud.

Overview

Therefore, strengthening digital competencies, critical thinking, and media awareness among young people is essential to promote safe internet use and responsible digital citizenship. These elements are central to fostering European digital resilience and supporting inclusive digital education within both formal and non-formal learning contexts.

Support and Reporting Channels

In Spain, several public bodies contribute to the prevention of online risks and the management of cyber incidents involving young people. The Spanish National Cybersecurity Institute (INCIBE) provides targeted guidance for minors and families through specialised online safety initiatives aimed at strengthening cybersecurity awareness, privacy protection, and responsible internet use. In addition, the national 017 cybersecurity helpline offers confidential assistance to individuals facing digital security concerns or online threats. Serious cybercrime cases may also be formally reported to national law enforcement authorities, including the Policía Nacional and the Guardia Civil.

Facebook Threat

Fake Copyright / Account Suspension Phishing



Main Platform

Facebook



Short Description

Users receive fraudulent messages claiming that their Facebook account or page has violated copyright or community standards. The message redirects them to a fake login page where credentials are collected. This phishing scheme frequently targets small businesses, associations, and young content creators in Spain.



Typical Youth Scenario

A young content creator receives a message claiming that their Facebook page has violated copyright rules and will be suspended. The message urges immediate action and includes a link to a fake verification page. The user enters their login credentials, after which the account is compromised and misused for fraudulent activities. The victim receives a message or post pretending to be from Facebook support.



How does it work?

The message claims a copyright or policy violation. A link redirects the user to a fake login or appeal page. The user enters login credentials and possibly verification codes. The attacker gains access to the account and misuses it.



Red Flags

Messages creating urgency about account suspension. Links that do not belong to official Facebook or Meta domains. Requests for passwords or verification codes via private messages. Messages from recently created or unverified accounts. Spelling mistakes or unusual formatting.



Prevention Tips

Verify account notifications directly within the official Facebook platform. Avoid clicking on suspicious links received via private messages. Enable two-factor authentication (2FA). Use strong and unique passwords. Participate in digital safety and cybersecurity awareness initiatives promoted by INCIBE or other national programmes.

Facebook Threat

Fake Copyright / Account Suspension Phishing



What to do if it happens?

Immediately change the account password.
Log out of all active sessions.
Use Facebook's official account recovery tools.
Report the fraudulent message through Facebook's reporting system. Contact INCIBE's 017 helpline for guidance if needed.



Severity

Likelihood 4/5 - This type of phishing is common on social media platforms in Spain and frequently targets pages managed by young users, associations, and small organisations.



Key Sources

Meta. (n.d.). Facebook Help Center – Security and login alerts. <https://www.facebook.com/help/>
Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). Phishing y fraudes online. <https://www.incibe.es/menores>

Instagram Threat

Influencer & Brand Impersonation Scams



Main Platform

Instagram



Short Description

Fraudulent Instagram accounts impersonate brands, public institutions, or influencers and contact users via direct messages with collaboration offers, fake giveaways, or account verification requests. These interactions often redirect users to phishing links or result in account takeover.



Typical Youth Scenario

A young Instagram user receives a direct message from an account claiming to represent a well-known brand or influencer offering a collaboration or giveaway prize. The message includes a link requesting account verification. Trusting the offer, the user enters login details or verification codes on a fake website. Shortly afterwards, the account is accessed and misused.



How does it work?

The victim receives a direct message from a fake brand or influencer account.

The message offers collaboration, prizes, or verification.

A link redirects the user to a phishing website.

The user enters login credentials or verification codes.

The attacker gains access to the account.



Red Flags

Messages offering collaborations or prizes from unverified accounts.

Accounts with slightly altered usernames of known brands.

Requests for login credentials or verification codes via DM.

Links directing to non-official Instagram or brand domains.

Urgent language pressuring immediate action.



Prevention Tips

Verify accounts through official brand or influencer profiles.

Avoid sharing login details or verification codes via direct messages.

Enable two-factor authentication (2FA).

Check usernames and account verification badges carefully.

Report suspicious accounts through Instagram's reporting tools.

Instagram Threat

Influencer & Brand Impersonation Scams



What to do if it happens?

Immediately change the Instagram password.
Log out of all active sessions.
Enable or reset two-factor authentication.
Report the fake account to Instagram.
Contact INCIBE (017 helpline) if further assistance is needed.



Severity

Likelihood 4/5 - Impersonation scams are common on Instagram in Spain, particularly affecting young users and emerging content creators.



Key Sources

Meta. (n.d.). Instagram Help Center. <https://help.instagram.com/>
Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). Suplantación de identidad y fraudes en redes sociales. <https://www.incibe.es/menores>

TikTok Threat

Fake Giveaways & Trending Challenge Scams



Main Platform

TikTok



Short Description

Scammers exploit viral TikTok trends and challenges by sharing links that promise prizes, free devices, or increased followers. These links redirect users to phishing websites or malicious applications outside the TikTok platform.



Typical Youth Scenario

A young TikTok user sees a viral video promoting a giveaway linked to a popular trend. The post promises a free smartphone or increased followers in exchange for quick registration. The user clicks the link in the bio or comments and is redirected to an external website requesting personal information or login details. Shortly afterwards, the account is compromised or personal data is misused.



How does it work?

1. The victim encounters a trending post or challenge promoting a prize.
2. The content includes a link in the bio, comments, or profile.
3. The link redirects to an external phishing website or app.
4. The user enters personal or account information.
5. The attacker collects the data or gains access to the account.



Red Flags

Offers of expensive prizes or rapid follower growth.
Links directing users outside the official TikTok platform.
Requests for login credentials or personal data.
Accounts recently created with few real interactions.
Urgent instructions to “act quickly” to claim rewards.



Prevention Tips

Verify giveaways through official brand or creator accounts.
Avoid clicking on suspicious links in comments or bios.
Enable two-factor authentication (2FA).
Do not download apps from unknown sources.
Report suspicious content through TikTok’s reporting tools.

TikTok Threat

Fake Giveaways & Trending Challenge Scams



What to do if it happens?

Immediately change the TikTok password.
Enable or reset two-factor authentication.
Remove any linked unknown applications.
Report the fraudulent content to TikTok.
Contact INCIBE (017 helpline) for additional guidance.



Severity

Likelihood 4/5 - Trend-based giveaway scams frequently appear on TikTok in Spain and disproportionately affect young users who actively engage with viral content and online challenges.



Key Sources

TikTok. (n.d.). TikTok Safety Center.
<https://www.tiktok.com/safety/pt-pt/>
Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). Fraudes y estafas en redes sociales. <https://www.incibe.es/menores>

Email Threat

Phishing Emails Impersonating Banks & Public Services



Main Platform

E-mail



Short Description

Fraudulent emails impersonate Spanish banks, tax authorities, or public services and request users to urgently confirm personal or financial information. These messages typically contain malicious links or attachments that lead to credential theft or malware installation.



Typical Youth Scenario

A young university student receives an email claiming to be from a Spanish bank or the tax authority regarding a refund or unpaid penalty. The message urges immediate confirmation of account details through a provided link. Believing it to be legitimate, the student enters personal or banking information on a fake website. Shortly afterwards, sensitive data is stolen, or the bank account is compromised.



How does it work?

1. The victim receives an email pretending to be from a trusted institution.
2. The message creates urgency (refund, penalty, blocked account).
3. A link or attachment redirects to a fake website or installs malware.
4. The user enters personal or financial data.
5. The attacker gains access to the victim's information or accounts.



Red Flags

Urgent requests to confirm data or avoid penalties.
Suspicious sender addresses not matching official domains.
Requests for banking details or verification codes.
Unexpected attachments or download prompts.
Generic greetings such as "Dear customer."



Prevention Tips

Verify information directly through official bank or government websites.
Do not click on suspicious links or open unexpected attachments.
Enable two-factor authentication (2FA) on financial accounts.
Keep antivirus and security software updated.
Never provide banking details via email.

Email Threat

Phishing Emails Impersonating Banks & Public Services



What to do if it happens?

Contact the bank immediately if financial data was shared.
Change passwords and activate 2FA.
Disconnect the device if malware is suspected.
Report the incident to INCIBE (017 helpline).
File a complaint with Policía Nacional or Guardia Civil if necessary.



Severity

Likelihood 5/5 - Phishing emails impersonating financial and public institutions are among the most widespread cyber threats in Spain and frequently lead to financial loss and identity theft.



Key Sources

Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). Fraudes y estafas en redes sociales. <https://www.incibe.es/menores>
Policía Nacional. (n.d.). https://www.policia.es/_es/index.php

Conclusions

The findings of this desk research indicate that phishing, impersonation schemes, and various forms of online fraud represent some of the most relevant cybersecurity threats faced by young people in Spain. These threats are especially significant because they occur on the platforms most used by youth, such as Instagram, TikTok, Facebook, and email, and rely heavily on social engineering techniques that exploit urgency, credibility, and emotional response. Given the high level of youth engagement in online communication, content creation, and academic activities, their exposure to deceptive links, fake accounts, and fraudulent messages is considerable.

For youth workers, these risks create an increasing need to enhance cybersecurity awareness, promote digital safety practices, and strengthen cyber resilience among young users. The identified risks reveal persistent gaps in privacy protection practices, understanding of data security, and the ability to critically assess digital content. Addressing these vulnerabilities requires structured youth-focused cybersecurity education that encourages responsible digital citizenship and safe internet use within both formal and non-formal learning contexts.

These findings directly support the objectives of the ESCAP(E+) project. Within the project framework and training materials, emphasis should be placed on phishing prevention, social engineering awareness, identity protection measures, and practical response strategies to cyber incidents. The development of VR escape game scenarios can simulate realistic online risk situations, allowing young participants to develop practical decision-making skills in immersive learning environments. Additionally, awareness materials such as infographics and animated videos should communicate key safety messages in a clear, engaging, and accessible format, reinforcing digital competencies and promoting inclusive digital education across diverse youth groups.

Conclusions

Through the integration of experiential learning approaches, innovative teaching methods, and targeted digital awareness campaigns, ESCAP(E+) has the potential to enhance European digital resilience and foster long-term improvements in cybersecurity awareness among young people in Spain.

Resources

- Instituto Nacional de Estadística (INE). (n.d.). Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares. https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528559&p=%5C&pagename=ProductosYServicios%2FPYSLayout
- Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). Ciudadanía. <https://www.incibe.es/ciudadania>
- Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). Menores – seguridad en internet. <https://www.incibe.es/menores>
- Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). El 017 se ocupa de la ayuda en ciberseguridad. <https://www.incibe.es/el-017-se-ocupa>
- Policía Nacional. (n.d.). https://www.policia.es/_es/index.php
- Guardia Civil. (n.d.). <https://web.guardiacivil.es/es>



ESCAP(E+)

Portugal

DESK RESEARCH



Co-funded by
the European Union

Overview

According to national education and digital statistics published by the Directorate-General for Education and Science Statistics (DGEEC) (1), young people in Portugal make frequent use of digital technologies in both academic and personal contexts. Internet access and digital devices are widely used for communication, information retrieval, learning activities, and social interaction.

Digital platforms play an important role in students' daily routines, including access to educational materials, participation in virtual learning environments, and maintenance of social connections. Social media and messaging applications are commonly used alongside formal digital learning systems, contributing to a highly connected and interactive digital lifestyle.

Mobile devices allow young people to remain constantly connected to online content and services. As a result, users frequently engage in private messaging, content sharing, and online collaboration across multiple platforms. However, limited verification of online information increases exposure to misinformation, fraudulent messages, and unsafe digital interactions. Overall, digital technologies create both opportunities and potential risks, making cybersecurity awareness essential within youth education and empowerment initiatives.

Key Risk Factors

According to the European Union Agency for Cybersecurity (ENISA), young people face several risk factors that increase their vulnerability to digital threats (2), including limited cybersecurity competencies, high exposure to social engineering strategies, extensive use of private messaging services, and limited understanding of data protection and privacy. These factors contribute to higher exposure to scams, impersonation attempts, and other forms of cybercrime.

Overview

Key National Indicators

Statistical data PORDATA (3) and Eurostat (4) indicate that internet use is widespread among young people in Portugal. Most users have regular access to digital technologies, although differences persist in digital competences and awareness of online safety practices.

Support and Reporting Channels

In Portugal, several national institutions provide support and reporting mechanisms for online risks, including CERT.PT, the Centro Nacional de Cibersegurança (CNCS), Linha Internet Segura, the Ministério Público Cybercrime Portal, and the Polícia Judiciária. These services contribute to safer digital environments and ensure access to trustworthy support for young people (5).

Footnotes:

1. Direção-Geral de Estatísticas da Educação e Ciência. (n.d.). DGEEC – Direção-Geral de Estatísticas da Educação e Ciência.
2. European Union Agency for Cybersecurity. (n.d.). *Awareness and cyber hygiene*.
3. PORDATA. (n.d.). *Base de Dados Portugal Contemporâneo*.
4. Eurostat. (n.d.). *Eurostat – Statistical Office of the European Union*.
5. CERT.PT (n.d.); Centro Nacional de Cibersegurança (n.d.); CISLab (n.d.); Ministério Público (n.d.); Polícia Judiciária (n.d.).

Facebook Threat

Fake Support Messages & Page Recovery Scams



Main Platform

Facebook



Short Description

Users receive fake messages claiming to represent Facebook support services and warning that their account or page may be suspended. The messages include links to phishing websites that request login details and security information.



Typical Youth Scenario

A young person managing a student association or community Facebook page receives a message claiming that the page has violated platform rules. The message warns of permanent deactivation within a short time. Concerned about losing access, the user clicks the link and enters login details on a fake recovery website. Shortly afterwards, the account is compromised and misused.



How does it work?

1. The victim receives a message pretending to be from Facebook Support.
2. The message claims that the account has violated platform policies.
3. A link redirects the user to a fake recovery or verification page.
4. The user enters their login credentials and security codes.
5. The attacker gains access to the account and misuses it.



Red Flags

Messages creating urgency about immediate account suspension. Links directing to websites that are not official Facebook or Meta domains.

Requests for passwords, verification codes, or personal information through private messages.

Messages sent from unknown or recently created accounts.

Spelling mistakes or unusual formatting in the message.



Prevention Tips

Verify security notifications directly through the official Facebook platform.

Avoid clicking on links received through private messages.

Enable two-factor authentication and use strong, unique passwords.

Regularly review account security settings.

Participate in digital safety and cybersecurity awareness training.

Facebook Threat

Fake Support Messages & Page Recovery Scams



What to do if it happens?

Immediately change the account password and log out of all sessions.
Use Facebook's official recovery tools to regain access.
Report the fraudulent message through Facebook's reporting system.
Inform followers or page members about the incident.
Contact national support services such as CERT.PT if needed.



Severity

Likelihood 4/5 - This type of scam is widespread on social media platforms and frequently targets users who manage pages or community accounts. Similar phishing attempts are regularly reported across Europe and in Portugal, making young users particularly exposed.



Key Sources

Meta. (n.d.). Protect your account from phishing and scams. <https://www.facebook.com/help/181495968648557>
Meta. (n.d.). Secure your Facebook account. <https://www.facebook.com/help/203305893040179>

Instagram Threat

Account Verification & Copyright Warning Scams



Main Platform

Instagram



Short Description

Users receive fraudulent messages claiming that their Instagram account will be removed due to copyright infringement or impersonation. The messages include links to phishing websites that request passwords and verification codes. The scam exploits users' fear of account suspension.



Typical Youth Scenario

A young content creator receives a message stating that their Instagram account has violated copyright rules. The message warns that the account will be removed within a short period. Worried about losing access, the user clicks on the link and enters login details on a fake verification page. Shortly afterwards, the account is compromised and misused.



How does it work?

The victim receives a message pretending to be from Instagram support.

The message claims a copyright or impersonation violation.

A link redirects the user to a fake verification website.

The user enters login credentials and security codes.

The attacker gains access to the account.



Red Flags

Messages warning of urgent account removal.

Links that do not belong to official Instagram or Meta domains.

Requests for passwords or verification codes.

Messages from unknown or recently created accounts.

Spelling or formatting errors.



Prevention Tips

Check security notifications inside the Instagram app.

Enable two-factor authentication.

Avoid clicking on links in private messages.

Use strong, unique passwords.

Review account security settings regularly.

Instagram Threat

Account Verification & Copyright Warning Scams



What to do if it happens?

Change the account password immediately.
Log out of all active sessions.
Use Instagram's official recovery tools.
Report the scam through Instagram.
Seek support from Linha Internet Segura if needed.



Severity

Likelihood 4/5 - This scam is common on Instagram, especially among young users and content creators. Similar phishing attacks are frequently reported in Portugal, making this threat highly relevant.



Key Sources

Meta. (n.d.). Instagram Help Center. <https://help.instagram.com/>
Safer Internet Centre Portugal. (n.d.). Internet Segura. <https://internetsegura.pt/>

TikTok Threat

Fake Monetisation & Creator Program Links



Main Platform

TikTok



Short Description

Users receive messages inviting them to join fake TikTok monetisation programmes or creator funds. These messages include links to external websites designed to collect login credentials or personal data. The scam exploits young users' interest in gaining visibility and financial rewards.



Typical Youth Scenario

A young TikTok user receives a message offering access to a monetisation or creator reward programme. The message promises financial benefits and increased visibility. Interested in growing their online presence, the user clicks on the link and enters personal and account information on a fake registration page. Shortly afterwards, the account is compromised and misused.



How does it work?

The victim receives a message offering access to a monetisation or creator programme. The message promises exclusive benefits or financial rewards. A link redirects the user to a fake registration website. The user enters login credentials and personal information. The attacker gains access to the account.



Red Flags

Messages promising easy money or exclusive creator programmes.
Links leading to websites outside official TikTok domains.
Requests for passwords or personal information.
Pressure to register quickly.
Messages from unknown or unverified accounts.



Prevention Tips

Verify monetisation information through the official TikTok app.
Avoid clicking on suspicious links.
Enable two-factor authentication.
Use strong and unique passwords.
Do not share personal data on external websites.

TikTok Threat

Fake Monetisation & Creator Program Links



What to do if it happens?

- Secure the account by changing the password and enabling two-factor authentication.
- Remove any suspicious linked emails, phone numbers, or devices.
- Review recent activity and delete unauthorized posts or messages.
- Report the fraudulent link or message through TikTok's safety tools.
- Submit an account recovery request if access is restricted.



Severity

Likelihood 3/5 - This scam mainly affects young and first-time content creators and appears regularly on TikTok. Although less widespread than email or social media phishing, it remains a relevant risk in Portugal.



Key Sources

TikTok. (n.d.). Centro de Segurança do TikTok (Portugal). <https://www.tiktok.com/safety/pt-pt/>
TikTok. (n.d.). Segurança da conta e do utilizador. https://support.tiktok.com/pt_BR/safety-hc/account-and-user-safety/account-safety

Email Threat

Invoice Fraud & Fake Delivery Notifications



Main Platform

Email



Short Description

Users receive fraudulent emails impersonating delivery companies, telecom providers, or service providers. These messages request payment, personal data, or attachment downloads. The scam aims to steal sensitive information or install malware on the user's device.



Typical Youth Scenario

A young person receives an email claiming to be from a delivery company about a missed package or unpaid invoice. The message includes a link or attachment requesting immediate action. Believing the message to be legitimate, the user clicks on the link or opens the file and enters personal or banking information. Shortly afterwards, sensitive data is stolen or malware is installed.



How does it work?

The victim receives an email pretending to be from a legitimate company.

The message requests urgent payment, document download, or verification.

A link or attachment redirects the user to a fake website or installs malware.

The user enters personal or financial information.

The attacker gains access to sensitive data or the device.



Red Flags

Emails creating urgency about payments or deliveries.

Unexpected attachments or download requests.

Sender addresses that do not match official company domains.

Requests for banking or personal information.

Generic greetings such as "Dear Customer".



Prevention Tips

Verify emails directly through official company websites.

Do not open suspicious attachments.

Avoid clicking on unknown links.

Use updated antivirus software.

Never share banking information by email.

Email Threat

Invoice Fraud & Fake Delivery Notifications



What to do if it happens?

Disconnect the device from the internet if malware is suspected.
Change passwords immediately.
Contact the bank if financial data was shared.
Report the email as phishing.
Run a full antivirus scan.
Seek support from CERT.PT or Linha Internet Segura.



Severity

Likelihood 5/5 - Email fraud is one of the most widespread cyber threats in Portugal and frequently targets young users. Similar scams are regularly reported, making this a highly relevant risk.



Key Sources

Safer Internet Centre Portugal. (n.d.). Internet Segura - Phishing e fraudes online. <https://cislabor.cncs.gov.pt/>
Polícia Judiciária. (n.d.). Cibercrime e burlas informáticas. <https://www.policiajudiciaria.pt/>

Conclusions

The findings of this desk research indicate that phishing, impersonation, and online fraud remain the most significant cybersecurity threats affecting young people in Portugal. These threats are especially common on social media platforms and through email communication, where users are frequently exposed to fraudulent messages, fake verification requests, and deceptive links. Given the strong presence of young people in digital environments for learning, communication, and social interaction, they are particularly exposed to such threats. As a result, youth workers are increasingly required to support young users in developing safer online behaviours and responding effectively to digital risks.

The analysis also demonstrates the importance of reinforcing digital literacy, critical thinking, and cybersecurity awareness among young people. Many of the identified threats exploit emotional pressure, lack of technical knowledge, and limited awareness of online security practices. These findings underline the need for structured educational initiatives that focus on phishing prevention, data protection, privacy awareness, and responsible digital citizenship. By strengthening these competencies, youth workers can contribute to building greater cyber resilience within both formal and non-formal learning contexts.

In response to these challenges, the ESCAP(E+) project should prioritise practical and engaging educational approaches. The project framework and training guidance should emphasise realistic examples, early risk detection, and effective response strategies. The development of VR escape game scenarios can provide immersive learning experiences that allow young people to practise decision-making in simulated cyber incidents.

Conclusions

In addition, awareness materials such as infographics and animated videos should communicate key safety messages in a clear, accessible, and visually engaging format. These resources can enhance digital inclusion and contribute to long-term improvements in cybersecurity awareness and online safety practices among youth.

Resources

- Direção-Geral de Estatísticas da Educação e Ciência. (n.d.). DGEEC - Direção-Geral de Estatísticas da Educação e Ciência. <https://dgeec.medu.pt/>
- European Union Agency for Cybersecurity. (n.d.). Awareness and cyber hygiene. <https://enisa.europa.eu/topics/awareness-and-cyber-hygiene>
- PORDATA. (n.d.). Base de Dados Portugal Contemporâneo. <https://pordata.pt/Portugal>
- Eurostat. (n.d.). Eurostat - Statistical Office of the European Union. <https://ec.europa.eu/eurostat>
- CERT.PT. (n.d.). Computer Security Incident Response Team Portugal. <https://cert.pt/>
- Centro Nacional de Cibersegurança. (n.d.). Centro Nacional de Cibersegurança. <https://cncs.gov.pt/>
- Centro Nacional de Cibersegurança. (n.d.). CISLab - Centro de Investigação em Segurança Digital. <https://cislabor.cnsc.gov.pt/>
- Ministério Público. (n.d.). Cybercrime portal. <https://cybercrime.ministeriopublico.pt/>
- Polícia Judiciária. (n.d.). Polícia Judiciária. <https://policijudiciaria.pt/>



ESCAP(E+)

CONCLUSION

Conclusions

This desk research shows that the most relevant cybersecurity threats affecting young people across the ESCAP(E+) partner countries are no longer mainly technical attacks, but social engineering threats embedded in everyday digital behaviour. Across Lithuania, Romania, Türkiye, Estonia, Spain, and Portugal, the strongest risks are linked to the platforms and communication channels that young people use most frequently, especially Instagram, TikTok, Facebook, messaging applications, and email. These threats include phishing, impersonation, fraud, identity misuse, misinformation, account takeover, and, in the most serious cases, sextortion and sexual blackmail.

At the same time, the research confirms that these risks take different forms depending on the national context. In Lithuania, youth are increasingly exposed to platform-specific scams that exploit local digital infrastructure such as Smart-ID, QR-based phishing, and trust in Facebook communities. In Romania, the main vulnerabilities are strongly behavioural and social, shaped by high screen time, peer pressure, scam funnels, cyberbullying, and rapid movement from social platforms to private messaging channels. In Türkiye, the risks are closely linked to mobile-first, highly visual, high-frequency online behaviour, where phishing, fake giveaways, impersonation, and misleading content are particularly effective. In Estonia, advanced digital integration does not reduce risk; instead, high connectivity increases exposure to disinformation, contact with strangers, manipulation, and severe harms such as sextortion. In Spain and Portugal, the research highlights phishing, impersonation, and online fraud as the most persistent and significant threats, particularly through social media and email.

A common finding across all partner countries is that young people's vulnerability is shaped less by lack of access to technology and more by patterns of use.

Conclusions

This means that cybersecurity education for young people cannot rely only on technical terminology or abstract warnings. It must be practical, relatable, youth-friendly, and directly connected to real online situations that young people encounter in their daily digital lives.

For youth workers, these findings underline the need for platform-specific and scenario-based cybersecurity education. Youth workers need tools that help them explain how scams actually work, how to recognise warning signs, and what to do immediately when an incident happens. Across the partner reports, several priorities emerge repeatedly: visual literacy, critical thinking, phishing recognition, account protection, safe use of privacy settings, two-factor authentication, identity protection, source verification, and knowledge of local reporting and support routes. The research also shows that emotional and social dimensions must be included, especially in relation to harassment, shame-based attacks, sextortion, and manipulation, where silence and stigma can prevent young people from seeking help.

These findings directly support the objectives of the ESCAP(E+) project and provide a clear foundation for the next outputs. First, the project framework and training guidance should emphasize practical digital resilience rather than only technical awareness. This includes recognising scam patterns, checking platform credibility, verifying identities and links, protecting accounts, understanding how personal data is exploited, and responding quickly and safely when risks appear. The framework should also help youth workers translate cybersecurity into non-formal learning settings using realistic examples and simple language.

Conclusions

Second, the desk research provides strong material for the development of VR escape game scenarios. The partner findings suggest that the most effective scenarios will be those based on realistic youth experiences, such as fake job recruitment, rental scams, hacked-account messages, fraudulent giveaways, QR-code phishing, fake delivery or customs fee requests, cloned profiles, misinformation chains, and sextortion or blackmail attempts. These scenarios can help young people practise recognition, decision-making, and safe response in immersive but controlled environments, which is fully aligned with the project's aim of using gamified and experiential learning methods.

Third, the findings also shape the direction of awareness content, including infographics, animated videos, and campaign materials. Across all countries, the evidence suggests that awareness materials should be short, visual, clear, accessible, and rooted in real platform behaviour rather than generic cyber language. They should highlight red flags, safe habits, immediate response steps, and local reporting options, while also promoting digital citizenship, inclusion, and confidence in seeking help. This is especially important for reaching young people with different digital skill levels and for ensuring that project outputs remain relevant and usable beyond the project period.

In conclusion, the combined partner findings confirm that youth cybersecurity in Europe must be addressed through a localised, practical, and educationally engaging approach. Although the specific threats differ across countries, the underlying pattern is shared: young people are exposed to manipulative, trust-based, and emotionally persuasive cyber risks through the platforms they use every day. By transforming these findings into a structured framework, immersive learning tools, and targeted awareness resources, ESCAP(E+) can make an important contribution to digital resilience, safer online behaviour, and the long-term strengthening of youth work in the field of cybersecurity education.



ESCAP(E+)

Stay tuned!

Stay connected for more resources and updates on our website.

<https://escapeerasmus.com/>



Co-funded by
the European Union