Online dangers

Cybercriminals use many different methods

You spend almost four hours a day on your smartphone. Apps like WhatsApp, games and social media help you stay connected — but 70% of young people encountered an online risk last year, such as suspicious messages or unsolicited “offers”.

Cybercriminals take advantage: tricking you so they can steal data, infect devices, or hack accounts. Their motive is typically money (e.g. through in-game purchases), blackmail, or fame.

In some instances, your data is sold on the dark web - don’t be an easy target!

Stealing data and identities

Stealing names, passwords, addresses and photos

Fraudsters try to collect personal information through social media, streaming platforms, grooming (adults pretending to be kids), or AI-generated deepfakes.

Tricking people

Scams using fake content and offers

Phishing emails, fake prize games, fake profiles, phone calls pretending to be “Customer support”, and trust scams – are all designed to trick you into clicking or giving away your login details.

Infecting devices

Installing spyware or trackers

Spyware can be installed through unknown apps, infected attachments/links, unsafe downloads, or by using public Wi-Fi without a VPN – all of which can expose your device to malware.

Hacking accounts

Breaking into accounts

Criminals exploit weak/reused passwords, “log in with social media” options, or stolen codes (e.g. for games, email, banking) – often followed by blackmail.

How to protect yourself

The best tips against cyber threats

Get help: talk to a trusted adult or contact a local support service.

Help & support
free and anonymous

Child Helpline International (global): 116 111
Find free, confidential child helplines (phone/chat) in 130+ countries. (https://childhelplineinternational.org/)

Safer Internet Centre (EU/Europe): Country-specific helpline + hotline for online issues (cyberbullying, grooming, illegal content, advice for families). (https://better-internet-for-kids.europa.eu/en/sic)

Quick tip: You can also report + block directly in many apps/platforms (Instagram, TikTok, WhatsApp, games).

01 | Strong passwords and MFA
Use a 20–25 character password/passphrase that's unique - try passkeys for even more security

02 | Protect your devices
Set up a PIN/biometrics and auto-lock, never leave devices unattended in public, update them regularly

03 | Avoid suspicious messages
Don't open unknown links/attachments — go directly to the known app or website instead

04 | Protect personal data
Don't send your address, other personal info or photos that you wouldn't want to be public

05 | Choose apps carefully
Download only from official stores, look out for fake shops, don't use untrustworthy sources

06 | Only use public WiFi in emergencies
Ideally only use public WiFi with a VPN-connection

07 | Spot fakes
Question AI answers, don't (re-)share deepfake content

08 | Use social media wisely
Set strong privacy settings, only add real friends, don't share locations — respect others' opinions

09 | Safer gaming
Avoid free-skin links, don't show/share private info in games or streams (through webcam)

10 | Trust your instincts
If there's pressure/bullying: involve parents/trusted adults or helplines, and change login details to affected accounts