



SMART ONLINE = SAFE OFFLINE

Stay safe online

The teen's guide: how to spot the traps, protect your accounts and know who to ask for help when something is not right.

Nicholas Carstoiu

Free guide for students in grades 7 to 12 · English edition · Updated October 2026

About this guide

This guide was written for you, not for specialists. You do not need to know how to code or love computers to understand it. Almost everything that follows is about people: the ones who try to fool you, the tricks they use and the small decisions, a few seconds long, that make the difference between a stolen account and a safe one. You can read it from start to finish or jump straight to the chapter you need; each one ends with a short **In short** section.

The guide grew out of SMART ONLINE = SAFE OFFLINE, the course I teach for free in Bucharest schools. Here I kept what matters most, checked every figure again and added the topics that have become important for teenagers: sextortion, fake images made with AI, chatbots, groups that demand “proof” and account theft through codes.

About the SMART ONLINE = SAFE OFFLINE programme

This guide is part of the free **SMART ONLINE = SAFE OFFLINE** programme that Nicholas Carstoiu offers to secondary schools and high schools in Bucharest, for students in grades 7 to 12. The programme is free for schools, students, teachers and parents. Details:

www.looksmart.ro/nicholas/projects/smart-online-safe-offline.html

The core course material was first developed by Alexandru Cârstoiu, an information security specialist, and adapted by Nicholas for teenagers.

The guide and the TRUST // NO TRUST platform work together. Here you find the explanations and steps you can keep at hand. On the platform you practise the decisions in fictional situations, before you need them for real. Both are free, so that access to safety information does not depend on being able to pay.

Every figure has its source written underneath, and the full list is at the end. If you find a figure that has changed in the meantime, write to me. Edition revised on the basis of the sources available on 23 October 2026. The help services listed are those available in Romania.

Do you need help right now?

112 if you or someone else is in immediate danger. **119** for abuse, exploitation or neglect of a child, free and around the clock. **116 111** if you want to talk to a counsellor. All services and steps are in [chapter 10](#). These are Romanian numbers; 112 and 116 111 also work in most EU countries.

Contents

	About this guide	2
	About the author	4
1	Why it matters	5
2	How attackers work	7
3	The classic traps	11
4	People who want to manipulate you	19
5	Your accounts and your phone	27
6	Safe gaming	31
7	Social media and your brain	35
8	Deepfakes and artificial intelligence	38
9	Viral scams	42
10	If it has happened to you	45
11	The trident: why the course belongs in schools	49
	Sources	50
	Contact, copyright and safety	53

About the author



Hi, I am **Nicholas Carstoiu** (Nicholas Cârstoiu). I am 17, in the 11th grade at the Romanian-Finnish High School in Bucharest, and I play competitive basketball for CSU ASE Bucharest. At my high school I am assistant coach of the junior teams.

Since 2023 I have been a member of the UNICEF Romania Children's Board, since 2024 a member of the Children's Advisory Council of Bucharest City Hall, and in 2026 I became Ambassador for Romania of United Citizens of Europe. Also in 2026 I received First Prize, "Young Leader in Volunteering", at the Romanian Social Volunteer Gala.

Online safety is not a new topic for me. I created the SMART ONLINE = SAFE OFFLINE programme, which I have been taking to Bucharest schools for three years, and The Fake News Factory, a media literacy project that won two awards in 2026. I am now building TRUST // NO TRUST, a free platform where teenagers practise the decisions that keep them safe, which I am entering in the Lider European 2026 competition.

"My generation doesn't have to be the easiest to fool online. We can be the hardest."

Get to know me better!

www.looksmart.ro/nicholas

CHAPTER 1

Why it matters

More and more of your life happens on a screen: friends, school, games, money, even first loves. That is exactly where people who want to take advantage of you go looking.

When you hear “cybersecurity”, you probably picture a hacker in a hoodie cracking passwords at lightning speed. Reality is much more ordinary, and that is precisely what makes it more dangerous. Many attacks do not start with a computer but with a person: a message that rushes you, a prize that is too good, a familiar voice on the phone, a new “friend” who understands you better than anyone else.

≈ 1 in 5

internet-using children aged 12 to 17, in 21 countries, experienced technology-facilitated sexual exploitation or abuse in a single year.

Source: UNICEF Innocenti, Through Children's Eyes report, published 3 September 2026, data from the Disrupting Harm research

1 in 6

students aged 11, 13 and 15, in 44 countries across Europe, Central Asia and Canada, experienced cyberbullying.

Source: WHO Europe, HBSC study on cyberbullying, 27 March 2024, data for 2022

2 in 5

children taking part in the Save the Children Romania study say they were insulted or received hurtful messages online.

Source: Save the Children Romania (Salvați Copiii), press release of 28 March 2025

More than 4 in 10

cases of technology-facilitated sexual abuse or exploitation, in the research summarised by UNICEF, were disclosed to no one.

Source: UNICEF Innocenti, Through Children's Eyes report, published 3 September 2026, data from the Disrupting Harm research

The last figure is perhaps the most important. Many problems grow precisely because they stay unspoken. If something happens to you, you do not need all the evidence or all the answers to ask for help. And if you recognise the trick in time and know what to do next, many of these things never get the chance to happen.

The **APDR** model: four questions that protect you

In this guide we use four simple questions, grouped under the name APDR. You can apply them to anything: an account, your phone, your photos.

1. Anticipate

What could go wrong? Who would want access to what I have?

2. Prevent

What do I do now so it does not happen?
Passwords, settings, caution.

3. Detect

How do I find out quickly if something has happened?

4. Respond

What do I do in the first minutes? Who do I tell?

Example: the photos on your phone

Anticipate: your phone can be lost or stolen, or someone may learn your code. Personal photos could reach people who should not see them. **Prevent:** you set an unlock code of at least 6 digits, turn on cloud backup protected by two-step verification and check which apps can access your gallery. **Detect:** you get an alert when someone signs in to your account from another device. **Respond:** you lock and wipe the phone remotely, change your cloud password and tell an adult.

Remember the order. Most people think about security only at step four, when the harm is already done. You can start at step one.

In short

- Many attacks rely on manipulating people, not only on technology.
- Problems that stay unspoken grow. Ask for help on day one.
- APDR: anticipate, prevent, detect, respond.

CHAPTER 2

How attackers work

Forget the lone hacker from the movies. Today's online crime looks more like a company, with teams, roles and deadlines.



Big attacks are carried out by teams, not by one person.

A cybercrime network works like a factory. Each team does one thing and does it well. If you understand the chain, you understand where it can be broken: very often, with you.

Profilers gather information about targets: what you post, where you go to school, your friends' names, the games you play. The **penetration team** looks for a way in, most often a phishing message or a reused password. The **attack team** installs malicious software or takes over the account. The **extraction team** copies the data, photos and contacts. **Negotiators** ask for money, and the “**clean-up**” team wipes the traces and sells the data on.

Not all hackers are criminals

The word “hacker” really means someone who understands a system so well that they can make it work differently from how it was designed. Some use that to steal. Others, called ethical hackers, look for vulnerabilities so they can be fixed before criminals find them. Big companies pay them through reward schemes called bug bounties.

Did you know?

In 2016, a 10-year-old boy from Finland, Jani, found a vulnerability that let him delete anyone's comments on Instagram. He reported it, and Facebook paid him 10,000 dollars. Cybersecurity is one of the few careers you can start very early, as long as you stay on the right side.

Source: NBC News, on the reward paid to a 10-year-old for an Instagram vulnerability, May 2016.

Did you know?

Romania has a serious tradition in security. Bitdefender, one of the best-known antivirus products in the world, was founded in Bucharest in 2001. And the RAV antivirus technology, developed by the Romanian company GeCAD, was bought by Microsoft in 2003.

Why would they care about you?

“I have nothing worth stealing” is the most common mistake. Your Instagram account can be used to fool your friends, your game account has skins that sell, your phone number opens WhatsApp accounts and your photos can be used for blackmail. To an attacker, it does not matter that you are “just a student”. What matters is that you have access to people who trust you.

The internet has three layers

The **surface web** is the part you find with Google: a restaurant's public page, an influencer's public profile, public YouTube videos. The **deep web** sounds mysterious, but it is simply everything behind a password: your inbox, private messages, your parents' bank account, your game library on Steam. There is nothing illegal there; it is your private space, and that is exactly what attackers want to get their hands on.

The **dark web** is a small part of the internet, reachable only through special software, where users' identities are hidden. It has legitimate uses too, for example for journalists in countries without freedom of expression. But it is also where stolen data, hacked accounts and much worse things are sold.



Why you have no business on the dark web

It is not a “cool” place to explore out of curiosity. You can stumble on illegal and traumatising content, download malicious software, and some sites are traps set by criminals or monitored by the police. If someone suggests going in “just to have a look”, the answer is no. If you see a link with illegal content involving a child, do not open it and report it anonymously to the esc_ABUZ line (chapter 10).

In short

- Online crime is organised like a business, with teams and roles.
- Some attacks are personalised with information about you, others are sent automatically to thousands of people. Either way, what you post matters.
- The deep web means your private accounts, not something illegal. The dark web is something else and is not a place to explore.
- You are not too young to be a target: you have accounts, contacts and other people's trust.

Exercise: how easily can a profiler find you?

Take five minutes and search for yourself on Google, with your full name in quotation marks. Then open your Instagram or TikTok profile as if you were a stranger. Write down everything someone who does not know you can find out: your school, your neighbourhood, the gym where you train, your parents' or sibling's names, your birthday, your daily routine.

Then ask yourself: if a stranger had all this information, what believable message could they send me? “Hi, I'm the new coach at the gym” or “Your form teacher was looking for you, here's the link to the new timetable” sounds far more convincing coming from someone who already knows details about you. That is how profilers work, and that is how you can protect yourself: the fewer clues you leave, the harder you are to fool.

How to spot a fake profile

- A new account with few posts, but many followers or many mutual friends added recently.
- Photos that are too perfect, model-style, or photos that also appear on other accounts (you can search them with Google Lens).
- It messages you first, praises you a lot and pushes to move to another app.
- It never accepts a video call or always has an excuse.

What to do now

- Make your account private wherever it does not need to be public.
- Remove your school, class and town from your bio if they are not needed.
- Do not post where you are in real time. Post after you have left.
- Check who follows you and remove accounts you do not know.

CHAPTER 3

The classic traps

Phishing, fake messages, calls that rush you and software that installs itself in secret. They are old, but they still work, because they keep adapting.



Phishing comes from “fishing”. The attacker casts a bait, an email, a text message or a social media message, and waits for you to bite. The message seems to come from someone you trust: a bank, a courier, Instagram, your school or a friend. It has a single goal: getting you to click, enter your password or a code, or download a file.

How to spot a phishing message

Almost all fake messages pull the same few psychological levers. Once you learn to feel them, it no longer matters how well the message is made.

Hurry

“Your account will be deleted in 24 hours.”
When you are rushed, you stop checking.

Fear

“Someone has logged in to your account.”
Fear makes you act without thinking.

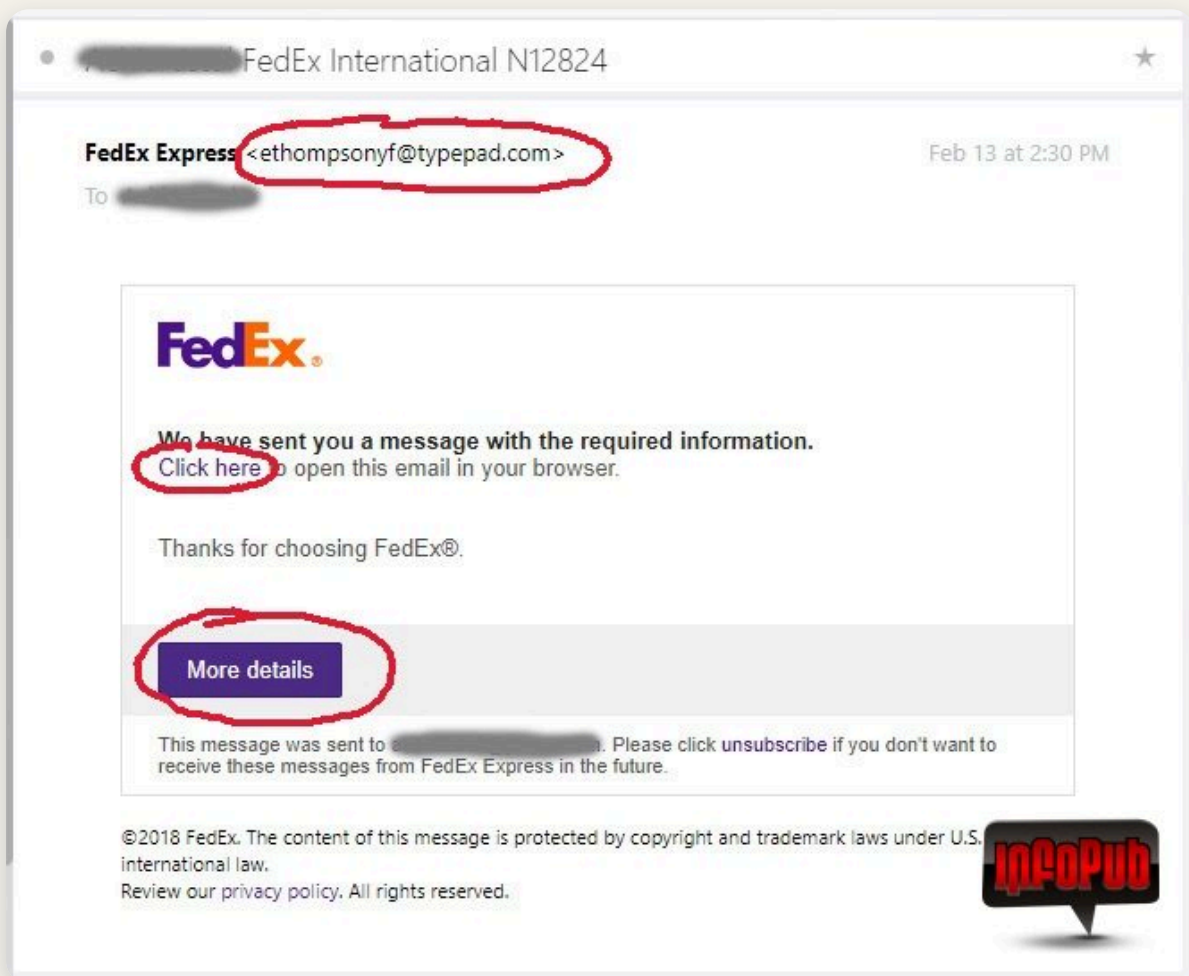
Curiosity

“Look at this photo of you going around.” You
want to see, so you click.

Gain

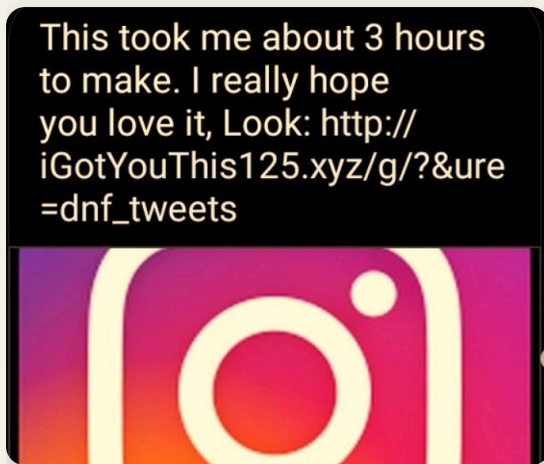
“You have won an iPhone.” If it sounds too
good to be true, it is not true.

Beyond the emotion, check three concrete things. First, the real address of the sender or the link, not the display name: a message “from FedEx” sent from an address like ethompsonyf@typepad.com is not from FedEx. Second, the domain: [instagram.com](https://www.instagram.com) is real, but [instagram-help.buzz](https://www.instagram-help.buzz) or [lgotyou125.xyz](https://www.lgotyou125.xyz) are not. Third, the request itself: no serious platform asks for your password or for a code received by text message in a message.



A real phishing example: the name says FedEx, the address says something else.

Is it an **attack** or not?



The message: “Took me about 3 hours to make. I really hope you love it. Look: <http://iGotYouThis125.xyz/g/?&ure=...>”, received privately from a friend.

Yes, it is an attack. The text is designed to make you curious, and the link sometimes even contains your username to look personal. The page it leads to looks like the Instagram login screen, but the domain is completely different. As soon as you enter your password, the account is taken over and the same message goes out automatically to everyone who follows you. That is why it seems to come from a friend: it really does come from their account, they just did not write it.

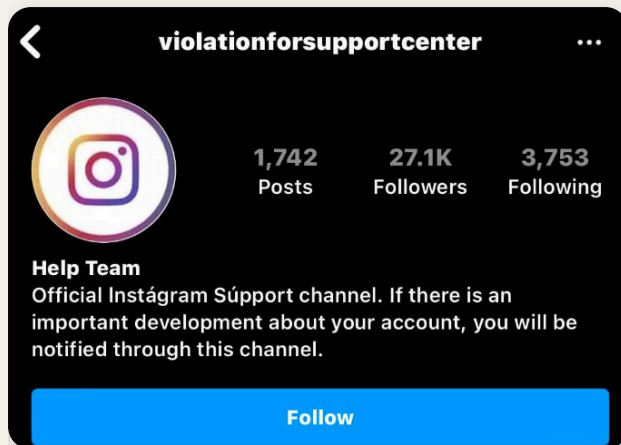
How to check a link without opening it

- On a computer, hover the mouse over the link and read the address that appears in the corner of the screen.
- On a phone, press and hold the link and read the address without opening it.
- Read the address between “https://” and the next “/”. A well-known name at the start does not mean the site belongs to it: in “instagram.com.account-check.example”, the domain is “account-check.example”, not “instagram.com”.
- If you are not sure, open the official app directly or type the address yourself instead of using the link.

What to do if you already clicked and entered your password

- Change the password of that account immediately, and of any other account where you used it.
- Turn on two-step verification.
- Go to Settings, Login Activity, and log out of sessions you do not recognise.
- Warn your followers not to click on messages sent from your account.
- If you can no longer get in, use the platform's official recovery page, not the “help” that messages you privately.

The “support team” that messages you first



A fake “Help Team” account, with the Instagram logo and thousands of followers.



“Last Warning: your account will be disabled.” The classic fear message.

An account presenting itself as the support team, with an official logo and big follower numbers, tells you that you broke the rules and must “confirm” your account through a link. Do not check the warning through the link you received. Open the app directly and look for the notification in the official security or support section.

Giveaways that collect your data



“Giveaway alert: like, tag 3 friends and share.” It looks harmless, but every step serves the person who created the giveaway. The **like** confirms you are an active account, so you can expect even more messages. **Tagging** exposes your friends, who become the next targets. **Sharing** sets the stage for other friends to be exposed too. Before you join in, check whether the organiser is the company's official, verified account.

Texts, calls and codes



Smishing means phishing by text message: “Your parcel is held, pay the 2 lei fee here.”

Vishing means phishing by voice call: someone claims to be from the bank, the police or your mobile operator and asks for details “for verification”. With artificial intelligence, the voice can even be that of someone you know (see chapter 8).

The golden rule of codes

A code received by text or in an app is the key to your account. **You never give it to anyone**, not to a “friend” who says they sent it to you by mistake, not to an “employee” of the bank or of WhatsApp. A real employee will never ask you for the code. If someone insists, it is an attack.

If you get a suspicious call, hang up and call back on the official number, which you find on the institution's website or on the back of the card. Do not call the number in the text message and do not tap the link you received.

Two traps that do not look like phishing

The QR code

A QR code can contain a link or the data for a specific action, and you cannot see what it contains before you scan it. It is not a proof of safety. Before you continue, read the address your phone shows you. Be very careful with QR codes you receive to “vote”, claim a prize or “confirm” your account: some are actually codes that link a stranger's device to your WhatsApp, Telegram or Discord account. Never confirm a device link that you did not start yourself.

The fake “I am not a robot” check

A real CAPTCHA check asks you to tick a box or pick some images. If a page asks you to open a command window, paste some text there and press Enter “to prove you are human”, stop immediately. It is a way of getting you to install malicious software yourself. In August 2026, Microsoft described a campaign that used exactly this kind of fake check.

Source: Microsoft Security Blog, TerminalFix campaign deploys a reverse tunnel through multistage intrusion, 28 August 2026.

If you have already run the command

- Disconnect the device from the internet.
- Ask an adult or a specialist to help you check the device.
- Change your important passwords from another, safe device, not from the affected one.



Software that installs itself in **secret**

Malware is the general name for any software made to harm you. It often reaches your device through a deceptive installation, when you think you are installing something else: a “cheat” for a game, a pirated app, a file received on Discord. But it can also get in through system vulnerabilities that have not yet been fixed by updates.

Type	What it does
Virus	Attaches itself to other files and spreads when you open them or send them on.
Trojan	Hides inside a program that looks useful, like the soldiers in the Trojan horse, and gives the attacker access to the device.
Spyware	Spies on you: what you type, which passwords you use, what messages you write, sometimes even the camera and microphone.
Ransomware	Locks or encrypts your files and asks for money to “give them back”.
Adware	Floods you with ads and pop-ups, many of them with dangerous links.



Did you know?

The first known ransomware appeared in 1989 and was handed out on floppy disks at an AIDS conference. More than 35 years later, in February 2024, a ransomware attack on the Hipocrate platform directly hit 26 hospitals in Romania, and dozens more were disconnected as a precaution. The attackers demanded 3.5 bitcoin, about 157,000 euros. Romania's cyber security directorate (DNSC) strongly advised against paying the ransom.

Source: TVR Info, on the attack on the Hipocrate platform, 13 February 2024.

How to **protect yourself** from malware

You do not need ten security programs. You need a few good habits, repeated until they become automatic.

- You install apps only from the official stores (Google Play, App Store) and games only from official platforms (Steam, Epic, the publisher's website).
- You do not download “cheats”, “generators” or “cracked” versions. They are the surest way to install a trojan yourself.
- You install system updates as soon as they appear. Many of them fix exactly the holes attackers use.
- You check what permissions an app asks for. A simple game does not need your contacts, microphone and location.
- You keep a backup of your important files, so that ransomware cannot blackmail you.
- If a message on the screen says you “have a virus” and must call or pay something, it is almost certainly a scam. Close the page and ask an adult for help.



In short

- Phishing catches you through hurry, fear, curiosity or gain.
- You check the real address, the domain and the request, not just the display name.
- You never give away codes received by text message.
- Malware can arrive through deceptive installations, but also through vulnerabilities. Updates and caution go together.

CHAPTER 4

People who want to **manipulate** you

The most painful attacks do not steal your password, they steal your trust. Cyberbullying, grooming, the loverboy method and sextortion run on emotions, not on technology.



Cyberbullying means humiliating, threatening, excluding or harassing someone through digital means: messages, comments, photos or clips shared without consent, groups created to laugh at someone, fake accounts. Unlike bullying in the schoolyard, online bullying follows you home, at any hour, and the audience can be huge.

Cyberbullying: how often it happens

49%

of the 4,449 students who answered a Save the Children Romania survey say they were victims of bullying. 27% admit they were aggressors.

Source: Save the Children Romania (Salvați Copiii), study on bullying in schools, press release of 18 October 2022

79%

of the same students say they witnessed bullying on social media, and 45% see cyberbullying often or very often.

Source: Save the Children Romania (Salvați Copiii), study on bullying in schools, press release of 18 October 2022

48.3%

of the children taking part in the study cited spend more than six hours a day in the digital environment.

Source: Save the Children Romania (Salvați Copiii), press release of 28 March 2025

45,245

reports (not victims or confirmed cases) of illegal or harmful online content involving children reached the esc_ABUZ line between 1 January and 3 December 2025.

Source: Save the Children Romania (Salvați Copiii), esc_ABUZ reporting line, press release of 10 December 2025

The 2022 Save the Children survey used a non-probability sample, so it shows a trend, not an exact measurement for all students in Romania.

What to do if you are the **target**

- Do not answer on the spot and do not take revenge. The bully is waiting for exactly that reaction.
- Save the evidence: screenshots of the messages, the account name, the date and time.
- Block the account and report it to the platform.
- Talk to an adult you trust: a parent, your form teacher, the school counsellor. It is not your fault and you do not have to carry this alone.
- If you receive threats of violence, it is a matter for the police, not just for the school.

What to do if you are a **witness**

Witnesses have more power than they think. Do not like, do not share and do not comment. Send a private message to the person targeted to say they are not alone. Report the post and tell an adult. One person saying “this is not OK” can change the mood of a whole group.

Grooming: the friend too good to be true

Grooming is the manipulation through which someone gradually wins the trust or submission of a child or teenager, often online, in order to abuse or exploit them. It does not look like danger. It looks like friendship: someone attentive who listens to you, praises you, gives you gifts in a game or offers you what you feel is missing.



The pattern repeats almost every time. First come the attention and the compliments. Then the conversation moves to a more private app, with the idea that “what we say stays between us”. Then the person tries to pull you away from your family and friends (“they don't understand you like I do”), and the requests become more and more personal. In the end there may be requests for photos, a proposal to meet or threats.

Warning signs

- An adult asking you to keep the conversation secret.
- Someone who wants to move the chat to a more hidden app.
- Gifts, money or virtual coins for no reason.
- Questions about your body or requests for photos.
- Pressure to meet, especially without anyone knowing.

Do not rely on the age someone claims: pressure and exploitation can also come from people you know or from people your own age. If you recognise one of these signs, stop the conversation, do not delete the text messages (they are evidence) and tell an adult straight away. You have done nothing wrong. The people who do this are skilled at manipulation and count precisely on your shame and silence.

“If you trust me, give me your password”

The risk does not only come from strangers. Sometimes it comes from someone you know well: a boyfriend, a girlfriend, a close friend. You do not have to prove love or friendship by giving access to your accounts, permanent location sharing or intimate images. Pressure, checking your phone, demanding passwords and threatening to publish something about you are signs of control, not of love.

Publishing your address, phone number or schedule to expose you is called **doxxing**. If it happens to you, keep the links and threats, report the posts and ask an adult for help. If your school or the gym where you train are involved, also tell a responsible adult there.

If you fear the person may become violent

Ask for help from a device the person has no access to. Plan password and location changes together with a trusted adult or a specialist: some of them can send notifications or be noticed. Your physical safety comes first. In immediate danger, call 112.

Source: eSafety Commissioner (Australia), non-consensual tracking, monitoring and harassment among children, updated 1 July 2025, survey from December 2024 to February 2025.

Consent to a photo is not consent to share it

The fact that someone sent you a photo or agreed to be photographed does not give you the right to pass it on. The rule applies between classmates and partners too, including when the image has been altered with AI. Whoever shares without consent does harm, even if “everyone has already seen it”.

If the first adult does not help you

Ask another adult for help: the school counsellor, a teacher, your coach or a child protection service. Do not give up because the first person ignored or blamed you.

The **loverboy** method



The “loverboy” method is one of the most common ways traffickers recruit girls, often minors. The trafficker makes the victim believe he has fallen in love with her. He promises a dream life, the emotional security she may not have at home, sometimes a move abroad “just for a while” to save money for their future together. Gradually the victim becomes emotionally dependent, then controlled, and the exploitation often begins with “do it for us, just once”.

6.3 million

people were, at any given time in 2021, in situations of forced commercial sexual exploitation. 1.7 million of them were children, and almost 4 in 5 victims are women and girls.

Source: International Labour Organization (ILO), Walk Free and International Organization for Migration (IOM), Global Estimates of Modern Slavery, September 2022

If your boyfriend, or a friend's, asks her to cut ties with her family, controls her phone, asks her for money or offers her a “job” abroad, talk to someone. In Romania, ANITP has a free line: **0800 800 678**.

Sextortion and fake images made with AI

Sextortion is blackmail with intimate images. An account that seems to belong to a girl or boy your age starts a conversation, flirts, sends a photo and asks for one in return. As soon as they get it, the tone changes: “Pay, or I send it to all your friends.” The attackers already have the list of your followers. They are fast, aggressive and, most of the time, organised networks from other countries who want money.

In recent years an even more cynical version has appeared: they no longer need a real photo. They take an ordinary picture from your profile and use artificial intelligence to create a fake image that looks intimate.

137 a day

In 2025, the US centre NCMEC received more than 50,000 reports of financial sextortion, an average of 137 a day.

Source: NCMEC, press release on sextortion, published 25 June 2026, data for 2025

More than 400,000

reports of child exploitation with a link to generative artificial intelligence were received by NCMEC in 2025.

Source: NCMEC, CyberTipline data, published 2026, data for 2025

These are reports received by a reporting centre, not the number of victims and not a measurement for Romania.

If it happens to you

- **Do not pay.** Paying does not guarantee the blackmail will stop and can lead to more demands.
- Stop the conversation. Keep the threatening messages and the account details. For intimate images, follow the rules in chapter 10.
- Block and report the account.
- Tell an adult. The blackmailer wants you alone and ashamed.
- For images, use [Take It Down](#) (next page) and Save the Children Romania's **esc_ABUZ** line. In Romania you can also call **119**.

You are not the one who did wrong. The crime is committed by the person blackmailing you.

What Take It Down can do

If you were under 18 when the intimate image was taken, you can use Take It Down for free (takeitdown.ncmec.org), even if you have since become an adult. The file must already be on your device: the image stays there, you do not send it to anyone, and the service only creates a digital fingerprint that participating platforms receive so they can block it.

Do not download the image and do not ask anyone to send it to you for this purpose. If you do not have it, ask for help by reporting: to the platform, the esc_ABUZ line, 119 or the police. The service can limit the spread, but it does not guarantee removal from the whole internet and does not work in all encrypted conversations. Report fake AI-generated images to the platform, to the esc_ABUZ line and to the police.

Source: NCMEC, Take It Down, frequently asked questions.

For parents: if your child tells you

Stay calm and thank them for telling you. The fact that they came to you is the most important thing. Do not look for someone to blame, do not take the phone away as a punishment and do not pay. Write down the account details and keep the threatening messages, without copying or forwarding the images. Report the account and ask for help from 119 or the police.

When a group asks you to **prove** something

Some online groups start with jokes, games or the promise that you finally belong somewhere. Europol warns that such communities look for victims on gaming and streaming platforms and on social media, then move the conversation to private channels. Then come the demands for “proof”: humiliate someone, send intimate images, hurt an animal, hurt yourself or harm someone else. They use threats or the information they have gathered about you to force you to continue.

You do not have to complete one last task

Do not rely on a promise that they will leave you alone after one more task. Stop the interaction and ask an adult for help. Keep the group's name and the threatening messages, without copying or sharing the abuse material. Do not investigate the group and do not try to confront it on your own. If there is immediate danger to you or anyone else, call 112.

Source: Europol, The rise of online cult communities dedicated to extremely violent child abuse, January 2025.

What victims **feel** and what helps them

People going through cyberbullying, grooming or sextortion usually feel the same mix: shame, fear, guilt and the sense that no one can help. That is exactly why attackers insist on secrecy. The most important thing you can do for yourself or for a friend is to break the silence.

For you

Talk to someone the same day. You do not need all the answers; it is enough to say “I have a problem and I need help”.

For a friend

Listen without judging, do not share anything they showed you and help them go to an adult. Do not promise to keep the secret if they are in danger.

For parents

Sudden mood changes, withdrawal, fear of the phone or, the opposite, being glued to it, falling grades. Ask calmly and do not take the phone away as a punishment.

For teachers

Treat every reported case as real, protect the student's identity and involve the school counsellor.



Romania's single national number 119: abuse, neglect or exploitation of a child. Free and around the clock.

In short

- Manipulation almost always looks like friendship, love or a compliment.
- Secrecy demanded by an adult is the clearest sign of danger.
- You never pay a blackmailer.
- The shame belongs to the aggressor, not to you.

CHAPTER 5

Your accounts and your phone

Passwords, two-step verification and a few well-chosen settings protect you more than any program. Here is what has changed in the rules about passwords.

Passwords: **length** beats complexity

You may have heard that a good password needs upper and lower case letters, numbers and symbols, and that it must be changed every few months. The rules have changed. The NIST guidelines of August 2025, a US standard for digital identity services used as a benchmark by specialists in many countries, say simpler things: length matters most, and forced changes at fixed intervals do not help.

Use a passphrase

Four or five unrelated words, for example “purple cactus jogs to Constanța”. It is long, easy to remember and hard to guess.

At least 15 characters

For accounts protected only by a password, NIST recommends a minimum of 15 characters.

One password per account

If a site is hacked, attackers try the same password everywhere. A reused password puts several accounts at risk at once.

Change it when needed

Not by the calendar, but when you have reason to believe it has been compromised.

Password	Why
Andrei2009	Weak: a name and a year, the first things an attacker tries.
M@r1aB3st!	Looks complicated, but it is short, and symbol tricks are well known to password-cracking software.
purple cactus jogs to Constanța	Good as an idea: long, unrelated to you, easy to remember. Do not use this exact one: it has appeared in a public guide.

What no longer works

Replacing letters with symbols (“p@ssw0rd”) does not fool password-cracking software, which knows all these tricks. Do not use your name, date of birth, your pet's name or strings like “123456” and “qwerty” either.

Source: NIST, SP 800-63B-4, Digital Identity Guidelines, August 2025.

Password managers and passkeys

Nobody can remember 40 different passphrases. That is why password managers exist: apps that generate, store and fill in passwords for you. You remember one very good one, and the app handles the rest. Phones and browsers already have built-in managers (Google Password Manager, Apple Passwords), and apps such as Bitwarden or 1Password do the same across all your devices.

Passkeys are the next step: a digital key tied to your phone, unlocked with your fingerprint, your face or your screen code. There is nothing to mistype on a fake site, and a passkey cannot be stolen through phishing the way a password can. If an account offers the option, turn it on.

Two-step verification

Two-step verification (2FA) asks, in addition to your password, for something only you have: a code from an app, a confirmation on your phone or a passkey. It greatly reduces the risk that a stolen password is enough to take over the account. It does not protect you from every attack, though: a fake site can ask you for the code too, and malicious software can steal a session in which you were already signed in. Choose passkeys or security keys when they are available. If you use codes, an authenticator app is generally better than text messages, but if text messages are the only option, turn them on: it is better than a password alone. Never approve a sign-in you did not start yourself. Turn on two-step verification first for your email, your main Google or Apple account, your social media, WhatsApp (two-step verification with a PIN) and your game accounts.

Source: CISA, Implementing Phishing-Resistant MFA (fact sheet); Microsoft, Token theft playbook.

The right order

1. Your main email: whoever controls it can reset the password of any other account.
2. Your phone's Google or Apple account.
3. WhatsApp, Instagram, TikTok, Snapchat.
4. Game accounts and platforms with money or saved cards.

Public Wi-Fi networks



Cafés, airports, hotels, shopping centres: free Wi-Fi is everywhere. Today most websites and apps encrypt data (the address starts with **https**), so connecting to a public network is usually safer than it was ten years ago. The danger remains with fake networks: anyone can create a network called “Free_Airport_WiFi”. Such a network can send you to fraudulent pages or ask you to install something. Simply connecting, however, does not automatically let whoever controls it read passwords and messages sent over properly encrypted connections.

Do not ignore your browser's security warnings and do not install certificates, apps or “updates” required to connect. HTTPS protects the connection to the site, but it does not prove the site is legitimate. A VPN does not turn a fake site into a safe one.

Source: FTC (United States), Are Public Wi-Fi Networks Safe? What You Need To Know.

Did you know?

When you turn on two-step verification, most platforms also give you **backup codes**. Store them somewhere safe, for example in your password manager or printed at home. They can help you get back in if you lose your phone. Check the platform's other recovery methods in advance too.

Simple rules for public Wi-Fi

- Ask the staff for the exact name of the network.
- For banking, payments or important passwords, use mobile data.
- Do not install anything and do not accept “updates” requested by the connection page.
- Turn off automatic connection to open networks.
- If you use public networks often, a VPN from a well-known company adds a layer of protection, but it does not replace paying attention.

Your phone, your **safe**

Your phone holds your photos, conversations, accounts, location and sometimes your card. It deserves to be protected like a safe.

Screen lock

A code of at least 6 digits, plus fingerprint or face unlock. Not 123456, not your year of birth.

Updates

You install system and app updates right away. Most of them fix security holes.

Permissions

Every month you check which apps can access the camera, microphone, location and contacts. You delete apps you no longer use.

Backup

Automatic cloud backup, protected by two-step verification.

Location and sharing

Limit which apps can access your location and check who can see where you are. Keep the settings your phone-finding service needs. Constant location sharing with other people should not be a condition of a friendship or a relationship.

Find my device

You turn on Find My (iPhone) or Find My Device (Android) before you need them.

Source: Google Account Help, Be ready to find a lost Android device.

From time to time, check on **haveibeenpwned.com** whether your email address has appeared in a data breach. If it has, change the password of that account and of any account where you used it.

If your phone is lost or stolen

1. You locate or lock it remotely from your Google or Apple account.
2. You change the password of your email and important accounts.
3. You ask your operator to block the SIM card, so nobody receives your codes by text message.
4. If necessary, you wipe the data remotely.

In short

- Long passphrases, one per account, kept in a password manager.
- Two-step verification everywhere, starting with your email.
- On public Wi-Fi you check the network, respect the security warnings and install nothing to connect.
- Phone locked, updated and backed up.

CHAPTER 6

Safe gaming

Games are among scammers' favourite places, because they are full of young people, virtual money and a lot of trust between players.



Your Fortnite, Roblox, Minecraft, Counter-Strike, League of Legends, EA Sports FC or NBA 2K account has real value: skins, coins, progress, sometimes a saved card. Scammers know this and have invented a few traps that repeat from one game to the next.

The traps that repeat in every game

Coin “generators”

Sites that promise free V-Bucks, Robux or coins in exchange for your login details. Real free rewards are only found in the game or on the official site.

Fake skins and trades

Trading or betting sites that look official but empty your inventory as soon as you log in.

Fake tournaments and events

Discord servers that promise prizes and ask for an “entry fee” or a login through a link.

Cheats and mods

Programs that promise you an advantage in the game but actually install a trojan or a program that steals your passwords.

Fake streams

Broadcasts that promise free skins to anyone who follows a link and logs in.

Buying accounts

You buy an account “with all the skins”, and the seller takes it back through password recovery. You can lose both the money and the account.

Did you know?

In January 2019, Check Point researchers showed that attackers could have taken over Fortnite accounts just by getting the player to click a link, without knowing the password. Epic Games fixed the problem, but the case showed that even the most popular game in the world can have holes.

Source: Check Point Research, Hacking Fortnite, 16 January 2019.

Watch out for “friends” in the game

In-game chat and Discord servers are also places where adults with bad intentions look for teenagers. The pattern is the one from chapter 4: attention, in-game gifts, moving the conversation to private, requests for photos or for “proof”. If someone you do not know in real life gives you skins or coins for no reason, ask yourself what they want in return.

When the game makes you **buy** one more time

Not all losses in games come from scammers. Some packs, chests or loot boxes give you random rewards: you pay without knowing exactly what you will get. Virtual coins make it harder to notice how much real money you have actually spent, and skins can end up on betting sites outside the game.

What to do

- You set a budget before you start and turn on confirmation for every purchase.
- You do not borrow money to win back what you lost.
- You do not use an adult's account to get around restrictions.
- If you hide your spending or keep going because “the next try has to work”, you stop paying and talk to an adult.

Source: eSafety Commissioner, How to manage money in games.

If your game account was stolen

1. Try recovery through the game's official support page, not through someone who messages you saying they can help.
2. Change the password of the email linked to the account.
3. Tell your in-game friends that it is not you messaging them.
4. If cards were saved, ask your parents to block them.



Safe gaming: five rules

- 1** Two-step verification on every game account. Epic, Roblox, Steam, Riot, EA and the others offer it for free.
- 2** Check “free” rewards in the game or on the official site. Do not give your password or codes to a middleman.
- 3** Never download hacks, cheats or generators. They are the surest way to lose your account and your computer.
- 4** Do not share your password with anyone. Not with your best friend, not with someone who promises to boost your rank.
- 5** Check every link before you click, especially those received on Discord or in the game chat.

For parents

Turn on parental controls on the console or account for spending and time limits, not for permanent surveillance. Do not save a card on the account without confirmation for every payment. And most importantly, play together from time to time: it is the simplest way to find out who your child talks to online.

In short

- A game account has real value and is a real target.
- “Free” offers outside the official game are usually bait.
- Loot boxes mean random spending: set yourself a budget.
- Cheats and generators bring malware.
- A generous stranger in the game wants something in return.

CHAPTER 7

Social media and your brain

The apps you use every day are built by very skilled people whose goal is to keep you in front of the screen for as long as possible.



Social networks help you stay in touch with friends and with relatives in other cities, show you things that interest you and save you from boredom. But they are also commercial products. The longer you stay, the more ads you see and the more money the platform makes. That is why real “attention engineers” work behind them, using behavioural psychology to make the app as hard to close as possible.

A little **chemistry**: why it is hard to stop

The brain has a reward system that motivates us to repeat the things that make us feel good. Dopamine plays an important role in this system, especially in anticipating a reward. Every like, every notification and every new clip can be a small reward, but you never know when the next one will come. This uncertainty, called variable reward, is the same mechanism that makes gambling so hard to quit.

In teenagers, the brain areas linked to reward are very active, while the areas involved in planning, decision-making and impulse control keep maturing into early adulthood. That does not mean you are “addicted” just because you like TikTok. It means it is normal to find it hard to stop, and it is worth building yourself a few brakes.

Source: National Institute of Mental Health (USA), The Teen Brain: 7 Things to Know.

The one-week experiment

Write down your screen time from your phone settings. Then, for one week, turn off social media notifications and leave your phone in another room at night. At the end, compare your screen time, your sleep and your mood. Many teenagers who try this are surprised by the result.

11%

of adolescents aged 11, 13 and 15 in 44 countries showed, in 2022, signs of problematic social media use (7% in 2018). Those who use it a lot but without losing control even report more support from friends.

Source: WHO Europe, HBSC study on teens, screens and mental health, 25 September 2024, data for 2022

Signs that social media **takes** more than it gives

- You go in “just for two minutes” and come out an hour later, without knowing where the time went.
- Your phone is the last thing you see at night and the first in the morning, and your sleep suffers.
- You feel irritated or restless when you have no internet access.
- You meet your friends in real life less and less.
- It hurts when you do not get the likes or comments you expected.
- You put off homework, training or sleep for one more clip.

How to take back control

Notifications

Turn them all off except messages from real people. You decide when you go in, not the app.

Time limits

Use Screen Time (iPhone) or Digital Wellbeing (Android) for daily limits.

Phone in another room

At night, the phone charges outside your bedroom. Sleep is the best upgrade you can give yourself.

A feed you choose

Unfollow accounts that make you feel worse. The algorithm learns from what you watch.

It is not just how long you stay, but what the content does to you

If an account pushes you to starve yourself, hurt yourself, hate a group or do something dangerous to be accepted, you do not have to keep following it. Neither the number of followers nor the fact that it appears in your feed makes it a safe source.

Use “Not interested”, block or report the account and look for the information in independent sources. Do not send a friend a traumatising clip to show them what you saw: you can ask for help by describing the situation. If it keeps affecting you, talk to an adult or a counsellor.

In short

- Apps are designed to keep you in front of the screen as long as possible.
- Unpredictable rewards make scrolling hard to stop.
- Turning off notifications and keeping the phone out of the bedroom make a huge difference.
- Content that hurts you gets blocked and reported, not shared.

CHAPTER 8

Deepfakes and artificial intelligence

What you see and hear is no longer proof in itself. A face, a voice or a clip can be created in minutes.



Deepfake joins two words: deep learning, the method by which computers learn from a huge number of examples, and fake. A deepfake is an image, a video clip or an audio recording altered or created with artificial intelligence, which looks or sounds like a real person. To make one, the software needs photos, clips and recordings of that person, and the more it has, the more convincing the result.

How it is used **against** people

Deepfakes can be used for jokes and films, but also to deceive, blackmail or destroy someone's reputation. Three important risks for teenagers are: fake intimate images created from ordinary photos (chapter 4), fake clips of well-known people recommending investments or giveaways, and calls in which a cloned voice of a family member urgently asks for money.

A real case

In 2024, an employee of the engineering firm Arup in Hong Kong took part in a video conference with the chief financial officer and other colleagues. All of them were fake, created with artificial intelligence. Convinced he was talking to real people, the employee transferred 200 million Hong Kong dollars, about 25 million US dollars, to the scammers' accounts.

Source: CNN, on the Arup deepfake fraud, 16 May 2024.

How to check, without relying only on **appearances**

Deformed fingers, impossible shadows, buttons that appear and disappear or lips out of sync may raise suspicion. Their absence, however, does not prove the image or recording is authentic. No AI detector should be treated as a final verdict: a study published by the UK government in 2026 shows that such tools perform worse in real conditions than in the lab.

Look for the original source, the date and the context. Check whether the information is confirmed independently. A real photo can be used with a fake story, and a generated image can look flawless. If the message asks for money, data, intimate images or urgent action, check with the person through a channel you already knew. Do not decide just because you recognised a face or a voice.

Source: Department for Science, Innovation and Technology (UK), Deepfake detection technology, 26 March 2026.

Checking a family emergency

Agree on a safety word that you never publish and never use in ordinary conversation. It is an extra clue, not a guarantee. If someone urgently asks for money, hang up and call the person on the number you already had saved. If they do not answer, check through another family member. Do not transfer money based only on a voice, a video call or the right answer to a single question.

Exercise: real or generated with AI?

The two images below are part of the REAL / FAKE / AI module of the TRUST // NO TRUST platform. We know exactly where they come from, because we created them for the exercise. Look at them as if you saw them in your feed, before reading the answer.



“BREAKING: the boulevard is a river right now!”

Answer: **AI-generated image made for this exercise.** We know this from its provenance. If you came across the post online, you would check the place, the date and independent confirmations. A lack of confirmations would mean the information remains unverified, not that you have proven AI was used.



“I'm giving away 10 phones, send me your

address!” Answer: **generated with AI;** this person does not exist. Skin with no texture can be a clue, but the message matters more: a stranger asking for your address in exchange for a prize is a trap, whether the face is real or not.

The lesson: we know these images are generated because we know where they come from. With an unknown post, separate two questions: “Is the image authentic?” and “Is the message credible?”. You do not need to prove AI was used to refuse a suspicious request.

In short

- An image or a voice is no longer proof in itself.
- The absence of flaws does not prove that something is real.
- You check the source and through another channel, especially when you are asked for money or data.

The AI that seems to **understand** you

A chatbot can explain a lesson or help you put an idea into words. But it can also be wrong, invent sources or give unsuitable advice, even when it answers very convincingly.

Some apps are built to seem like friends or partners. The fact that they answer you with empathy does not mean they know you, have feelings or can take care of you.

32%

of Australian children aged 10 to 17 who had used an AI assistant or companion said they had shared personal or sensitive information with it, including photos or secrets. The survey covered almost 2,000 children.

Source: eSafety Commissioner (Australia), Talking to machines, report published August 2026, survey carried out in 2026

What you do not tell a chatbot

- Passwords, codes, ID details, your address.
- Intimate images, of yourself or of anyone else.
- Other people's private conversations.

Do not assume the conversation is as confidential as a session with a psychologist. Check the service's settings and rules on keeping and using data.

If conversations with a chatbot start to replace your sleep, your friends or help from people, talk to someone you trust. For abuse, blackmail, health or danger, ask an adult or a professional for help. Do not let a chatbot be your only support.

You can practise more in the REAL / FAKE / AI module of the TRUST // NO TRUST platform, where you choose between real photos, edited images and images generated entirely by AI.

CHAPTER 9

Viral scams

Some scams do not look like attacks but like favours: a vote for a friend's daughter, an easy job from home, a prize from a well-known shop.

“Please **vote** for Adeline”

Bună, ați putea vota pentru Adeline aici, vă rog? Aceasta este fiica prietenilor mei. Școala organizează un concurs pentru ei, al cărui premiu este grantul educațional al anului. Vă mulțumesc foarte mult pentru ajutor!

<https://dancingvot.top/home/vote1>

18:03

The message arrives on WhatsApp, usually from someone you know: “Hi! Please vote for Adeline in this poll, she is my friend's daughter, the main prize is a study scholarship. Thank you so much!” The link leads to a site with two girls and a vote button. (The screenshot is a real example from Romania.)

When you press “Vote”, a window asks for your phone number and then for the code you have just received on WhatsApp. You think you have voted. In reality, you have entered the code that links a new device, and the attackers now have access to your WhatsApp account. Straight away, the same message goes out to all your contacts, and sometimes your account is suspended for spam.

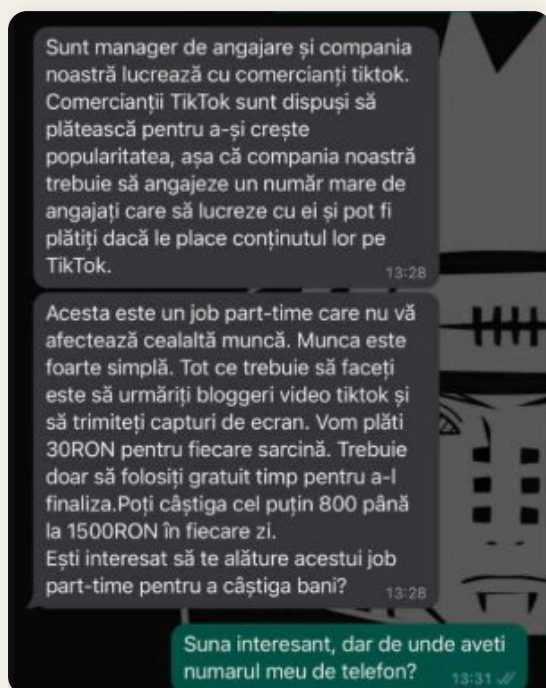
How to protect yourself

- You do not enter a code received on WhatsApp into a page opened from a message.
- You turn on WhatsApp's two-step verification: Settings, Account, Two-step verification.
- You regularly check Settings, Linked devices and log out of anything you do not recognise.
- If a friend asks you for something unusual, you call them.

Same trick, different clothes

- **The hurried buyer** on a classifieds site who sends you a link “so you can receive the money” and asks for your card details.
- **Concert tickets** sold by “someone who can no longer make it”, paid in advance and never received.
- **The courier text** asking for a small fee for a parcel you never ordered.

The work-from-home job that **costs** you



“Interested in a part-time job? You like TikTok clips and get 30 lei (a few euros) for every screenshot. You can earn 800 to 1,500 lei a day.” At first you really do receive a few lei, so you start to trust them. Then you are asked to “invest” a sum to unlock better-paid tasks. That money never comes back.

The channel they contact you on does not prove the offer is real. Check the employer independently and never pay to receive your wages or to unlock tasks.

What do you give **in return**?



Giveaways with big prizes, gifts from well-known shops, apps that show you “what you will look like in 30 years” and quizzes that tell you “which character you are” often have a hidden price: your data, your contacts or access to your account. Not everything free is a trap, and this guide is an example. Before you accept something, ask yourself what you give in return and who receives it.

Your account is not a **transfer** service for others

“You get some money in your account, send it on and keep a commission.” It may look like a simple job or a favour for a friend. In reality, you can be used to move money that comes from fraud. Europol describes this scheme as **money muling**, a form of money laundering, and the person who receives and transfers the money for someone else is called a “money mule”.

What to do

- You do not lend access to your bank account and do not open accounts for someone else.
- You do not hand over your card, codes or photos of your ID for an unchecked offer.
- If the money has already arrived, you do not withdraw it and do not send it on as instructed by whoever contacted you.
- You tell your bank immediately, tell an adult and ask the police for guidance. You keep the conversation and the transfer details.

Source: Europol, prevention guide on money muling.



In short

- Codes are used only in the official procedure you started yourself; you do not share them and do not enter them on pages received for votes or prizes.
- A small payment at the start does not prove the job is real. You do not send money to continue or to withdraw supposed earnings.
- A job that asks you for money to start is a scam.
- Your bank account is not for lending.

CHAPTER 10

If it has happened to you

Anyone can be fooled, including adults and specialists. What matters is what you do in the first minutes, and not staying alone with the problem.

- 1 Stop.** Do not reply, do not click, do not pay anything. Breathe. The attacker is counting on your panic.
- 2 Keep the evidence without spreading the abuse.** Write down the account name, the link to the profile or post, the date and time. Keep threatening messages and demands for money. If sexual images of a minor are involved, do not download, copy or forward them “as evidence”: ask the police or the reporting service for instructions. Do not delete messages or your account in a panic.
- 3 Tell an adult you trust.** A parent, your form teacher, the school counsellor, your coach. Today, not tomorrow.
- 4 Secure your accounts from a safe device.** Change your passwords, starting with your email, check the recovery methods and close unknown sessions. If you installed something suspicious, do not enter new passwords on the affected device. Follow the steps for your situation on the next page.
- 5 Report.** To the platform (the Report button), then to the right institutions, on the following pages.
- 6 Take care of yourself.** What you feel is normal. If it weighs on you, talk to a counsellor, for example on 116 111.

What not to do

- Do not pay and do not send more photos or details, however much you are pressured.
- Do not take revenge and do not threaten back.
- Do not delete conversations or your account in a panic.
- Do not pay someone who promises to recover your account for a fee, and do not give them access to your phone or codes.
- Do not try to sort it out alone. Online problems are solved faster with an adult beside you.

The first step depends on **what happened**

You entered your password on a fake site

From a safe device, go directly to the official app or site, change the password and close unknown sessions. Check the recovery methods (email, phone) and connected apps. If the password was used elsewhere too, change it there as well.

You gave your card details or sent money

Contact the bank immediately, through the official app or the number on the back of the card, and ask a parent or trusted adult for support. Ask for the card to be blocked and the transactions to be checked. Do not wait for an answer from a reporting site.

You installed something suspicious or ran a command

Disconnect the device from the internet and ask for technical help. Do not enter new passwords on it until it has been checked. Change your important passwords from another device.

You are being blackmailed with images

Do not pay, do not send more material and ask an adult for help. Keep the threatening messages without spreading the images. Use Take It Down, esc_ABUZ or 119.

Someone promises recovery for a fee

Do not give them access to your phone, money or codes. Use only the platform's official recovery and the institutions on the next page.

Source: Microsoft, Token theft playbook.

Where to get **help** in Romania

112

Emergencies. Call if someone is in immediate danger or you are threatened with violence.

119

Child protection: abuse, neglect or exploitation of a child. Free, around the clock, and you can ask to stay anonymous.

116 111

Telefonul Copilului (child helpline): you talk to a counsellor. Free from Orange, Telekom and Vodafone, Monday to Friday, 10:00 to 20:00, or write to vorbestecunoi@telefonulcopilului.ro
Current hours:
telefonulcopilului.ro

0744 360 446

Ora de Net helpline (Save the Children Romania): questions about online safety, 10:00 to 17:00. Current contact details:
oradenet.ro/helpline

esc_ABUZ

Save the Children Romania reporting line for illegal content involving children. You can report just the link, anonymously:
oradenet.ro/linia-de-raportare

Take It Down

NCMEC: helps remove intimate images of minors from participating platforms, without sending the image. Available worldwide:
takeitdown.ncmec.org

1911

DNSC: phishing, hacked accounts and online fraud. You can also write to alerts@dnsc.ro

0800 800 678

ANITP, human trafficking: free call within Romania. From abroad: +40 21 313 31 00.

Police

Ask the police for help. If you can, go with a trusted adult, but do not put off asking for help if you have no one with you right away. In an emergency, call 112.

Sources and contact pages: 112.ro, servicii publice.gov.ro, edupedu.ro (launch of 119), telefonulcopilului.ro, oradenet.ro, takeitdown.ncmec.org, dnsc.ro, anitp.mai.gov.ro. Information checked in October 2026; hours and conditions may be updated by each service.

When you call or write, prepare

What happened and when, the names of the accounts involved, the links and the threatening messages. For intimate images, make no copies: follow the rule in step 2. You do not need to have everything. Say what you know, and the people at the other end will help you with the rest.

Need help with other situations? The HELP module on the TRUST // NO TRUST platform asks you what happened and shows you exactly who to turn to.

What to remember from **this guide**

Your mind

- Unspoken problems grow: you ask for help on day one.
- Hurry, fear, curiosity and gain are warning signs.
- If it sounds too good to be true, it is not true.
- An image or a voice is no longer proof in itself.

Your accounts

- Long, different passphrases, in a password manager.
- Two-step verification, starting with your email; you do not approve sign-ins you did not start.
- Codes received by text or WhatsApp are given to no one.
- Passkeys wherever they are available.

Your devices

- Updates as soon as they appear.
- Apps only from the official stores.
- No cheats, generators or pirated software.
- Backup and location turned on.

People

- Someone who asks you to hide pressure, intimate requests or threats is a sign of danger.
- You never pay a blackmailer.
- You do not share or like someone else's humiliation.
- You ask for help on day one. The shame belongs to the aggressor.

The 10-second test before any click

1. Who is really writing to me? The real address, not the display name.
2. Is it rushing me, scaring me or promising me something?
3. Is it asking for a password, a code, money or a photo?
4. Can I check through another channel, by calling or going directly into the app?
5. Do I have the consent of the person concerned, and do I understand what could happen to this content?

You may come across fraud attempts even when you are careful. Being prepared helps you recognise them and limit the consequences.

CHAPTER 11

The trident: why the course belongs in schools

Online safety is not built only inside a teenager's phone. It needs three prongs working together: students, parents and teachers.

Students

They learn to recognise manipulation through real examples from their own lives: Instagram, WhatsApp, games, TikTok. They share a common language with their classmates, so that “that’s phishing” or “don’t give the code” becomes a group reflex. They find out where to get help before they need it and learn that they are not alone, which reduces shame and silence, exactly the attackers’ weapons.

Parents

They understand the real risks, not those from the headlines, and get the signs to watch for. They learn how to talk to their child without scaring them and without taking the phone away as a punishment, which would make the child hide the next problem. They can secure the family’s accounts and agree together on rules and a safety word.

Teachers

They get ready-to-use material for form periods, IT or social education classes, and a way to recognise and handle cases of cyberbullying or grooming. The school becomes a place where students report instead of hiding.

The TRUST // NO TRUST platform includes exercises and an educational assessment tool, CDRS, which is in development and piloting. The results can show which answers students have mastered and which topics need revisiting. The score is not a diagnosis and does not guarantee that a student or a school is protected from incidents.

When the three prongs work together, a teenager is no longer alone in front of a screen. They have classmates who recognise the same tricks, parents who know what to ask and teachers who know what to do. That turns a lesson of a few hours into a culture of safety.

Bring the course to your school

SMART ONLINE = SAFE OFFLINE is free for schools, students, teachers and parents. A session lasts one day, in a room with a projector, and needs no special equipment. It is currently taught in Romanian, in Bucharest schools. To book a session, write to nicholas.carstoiu@gmail.com or call +40 743 332 318.

Sources

Every figure in this guide was checked against its source in October 2026. The sources include reports, press releases and official pages. Where it matters, the publication date is kept separate from the period the data refers to.

1. UNICEF Innocenti, Through Children's Eyes report, published 3 September 2026, data from the Disrupting Harm research.
<https://www.unicef.org/innocenti/reports/through-childrens-eyes>
2. WHO Europe, HBSC study on cyberbullying, 27 March 2024, data for 2022.
<https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study>
3. WHO Europe, HBSC study on teens, screens and mental health, 25 September 2024, data for 2022.
<https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health>
4. National Institute of Mental Health (USA), The Teen Brain: 7 Things to Know.
<https://www.nimh.nih.gov/health/publications/the-teen-brain-7-things-to-know>
5. Save the Children Romania (Salvați Copiii), study on bullying in schools, press release of 18 October 2022.
<https://www.salvaticopiii.ro/sites/ro/files/2023-11/studiu-pestre-un-sfert-dintre-copii-au-fost-agresori-jumatate-spun-ca-au-fost-victime-ale-bullying-ului.pdf>
6. Save the Children Romania (Salvați Copiii), press release of 28 March 2025.
<https://salvaticopiii.ro/sites/ro/files/2025-03/5-ani-a-scazut-pragul-de-varsta-pentru-copii-pe-retele-sociale-avertisment.pdf>
7. Save the Children Romania (Salvați Copiii), esc_ABUZ reporting line, press release of 10 December 2025.
<https://www.salvaticopiii.ro/sites/ro/files/2025-12/expunere-si-continut-daunator-copii-online-crestere-alarmanta-a-sesizarilor.pdf>
8. NCMEC, press release on sextortion, published 25 June 2026, data for 2025.
<https://www.missingkids.org/blog/2026/ncmec-releases-new-sextortion-data-2025>
9. NCMEC, CyberTipline data, published 2026, data for 2025.
<https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata>
10. NCMEC, Take It Down, frequently asked questions.
<https://takeitdown.ncmec.org/faq/>
11. Europol, The rise of online cult communities dedicated to extremely violent child abuse, January 2025.
https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The_rise_of_online_cult_communities_dedicated_to_extremely_violent_child_abuse.pdf
12. eSafety Commissioner (Australia), non-consensual tracking, monitoring and harassment among children, updated 1 July 2025, survey from December 2024 to February 2025.
<https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia/snapshot-non-consensual-tracking-monitoring-harassment>

Sources (continued)

13. eSafety Commissioner (Australia), Talking to machines, report published August 2026, survey carried out in 2026.
<https://www.esafety.gov.au/research/talking-to-machines-childrens-experiences-with-ai-assistants-and-companions>
14. Europol, prevention guide on money muling.
<https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling>
15. NIST, SP 800-63B-4, Digital Identity Guidelines, August 2025.
<https://pages.nist.gov/800-63-4/sp800-63b.html>
16. CISA, Implementing Phishing-Resistant MFA (fact sheet).
<https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>
17. Microsoft, Token theft playbook.
<https://learn.microsoft.com/en-us/security/operations/token-theft-playbook>
18. FTC (United States), Are Public Wi-Fi Networks Safe? What You Need To Know.
<https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know>
19. Microsoft Security Blog, TerminalFix campaign deploys a reverse tunnel through multistage intrusion, 28 August 2026.
<https://www.microsoft.com/en-us/security/blog/2026/08/28/terminalfix-campaign-deploys-reverse-tunnel-through-multistage-intrusion/>
20. Department for Science, Innovation and Technology (UK), Deepfake detection technology, 26 March 2026.
<https://www.gov.uk/government/publications/deepfake-detection-technology/deepfake-detection-technology>
21. International Labour Organization (ILO), Walk Free and International Organization for Migration (IOM), Global Estimates of Modern Slavery, September 2022.
<https://www.ilo.org/publications/major-publications/global-estimates-modern-slavery-forced-labour-and-forced-marriage>
22. TVR Info, on the attack on the Hipocrate platform, 13 February 2024.
<https://tvrinfo.ro/blocajul-generat-de-atacul-cibernetice-asupra-spitalelor-continua-hackerii-au-cerut-o-rascumparare-de-peste-150-de-mii-de-euro-in-bitcoin/>
23. CNN, on the Arup deepfake fraud, 16 May 2024.
<https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk>
24. Check Point Research, Hacking Fortnite, 16 January 2019.
<https://research.checkpoint.com/2019/hacking-fortnite/>
25. NBC News, on the reward paid to a 10-year-old for an Instagram vulnerability, May 2016.
<https://www.nbcnews.com/tech/social-media/facebook-pays-10-000-10-year-old-instagram-hacker-n568026>

Sources (continued)

26. Google Account Help, Be ready to find a lost Android device.
<https://support.google.com/accounts/answer/3265955?hl=en>
27. eSafety Commissioner, How to manage money in games.
<https://www.esafety.gov.au/parents/issues-and-advice/gaming/how-to-manage-money-in-games>
28. TRUST // NO TRUST, the REAL / FAKE / AI module (AI-generated images made for the exercise).
<https://www.looksmart.ro/trustnotrust/real-fake-ai/>
29. DNSC, Romania's National Cyber Security Directorate, number 1911 for reporting incidents.
<https://www.dnsc.ro/>
30. Have I Been Pwned, checking for compromised email addresses.
<https://haveibeenpwned.com/>
31. Ora de Net, Save the Children Romania: helpline and esc_ABUZ reporting line.
<https://www.oradenet.ro/linia-de-raportare/>
32. Telefonul Copilului Association, how 116 111 works.
<https://telefonulcopilului.ro/116111/afla-cum-functioneaza-telefonul-copilului-116111/>
33. Romanian public services portal gov.ro, social assistance and child protection (119).
<https://serviciipublice.gov.ro/servicii?domainSlug=asistenta-sociala-si-adoptii>
34. Edupedu, on the launch of the 119 number, 5 January 2022.
<https://www.edupedu.ro/cazurile-de-copii-abuzati-pot-fi-semnalate-la-numarul-de-telefon-unic-national-gratuit-119-numa-rul-este-corelat-cu-112-si-echipe-mobile-pot-intervenii-imediat/>
35. ANITP, Romania's National Agency against Trafficking in Persons.
<https://anitp.mai.gov.ro/contact/>
36. Romania's Single National Emergency Call System 112.
<https://www.112.ro/>
37. The SMART ONLINE = SAFE OFFLINE programme.
<https://www.looksmart.ro/nicholas/projects/smart-online-safe-offline.html>
38. The TRUST // NO TRUST platform.
<https://www.looksmart.ro/trustnotrust/>

About the images

The chapter illustrations come from the SMART ONLINE = SAFE OFFLINE course materials and were created with the help of artificial intelligence. The screenshots of fraudulent messages are reproduced solely for educational purposes, to help readers recognise fraud; several of them are real examples received in Romania. The trademarks and logos visible in them belong to their owners, who have nothing to do with those messages. The two images in the chapter 8 exercise were generated with AI for the REAL / FAKE / AI module of the TRUST // NO TRUST platform.



Better **safe** than sorry

You have finished the guide. Now practise: the TRUST // NO TRUST platform puts you in fictional situations, inspired by real risks, where you decide for yourself what to do.

www.looksmart.ro/trustnotrust

CONTACT

Nicholas Carstoiu

nicholas.carstoiu@gmail.com · +40 743 332 318

www.looksmart.ro/nicholas

Copyright. © 2026 Nicholas Carstoiu (Nicholas Cârstoiu). All rights reserved. This guide may be downloaded, printed and distributed free of charge, in full and without changes, for non-commercial educational purposes, with the source credited. Selling, modifying or reproducing parts of the content without the author's written consent is prohibited.

About safety. This guide is for information and education only. Following its recommendations reduces risk, but does not guarantee protection against every online threat, as threats change constantly. The guide is one brick in your digital education, not a substitute for talking to parents, teachers or specialists. In any dangerous situation, contact 112 immediately or the help services in chapter 10.