



**Online Safety
Protection from Scams**

We live in an increasingly connected world, where chatting, buying, selling, or meeting new people is just a click away. But it's not all sunshine and roses: the internet itself hides many risks, with scammers ready to deceive us.

This guide is designed for you—boys and girls—who use your phone every day, are active on social media, or shop online. It will help you recognize the most common scams, such as fake shopping websites, romance scams, fraudulent bank messages, or cryptocurrency scams.

Simple, straightforward, and full of practical examples, this guide will teach you how to protect yourself, when to be suspicious, and what to do if you feel threatened.

Because safe browsing is the first real line of defense. And remember: even a single click can make a difference.



Electronic commerce

This is the most widespread online scam and it affects both buyers and sellers.

The most common forms are three:

- **1. Fake e-commerce websites**

Websites that look legitimate, filled with products at very attractive prices.

After paying via bank transfer or card, the goods never arrive.

The seller disappears and the contact details are fake or nonexistent.

Sometimes you receive a cash-on-delivery package, pay upon delivery, but inside there are items of very little value.

- **2. Fake listings on platforms such as Subito, eBay, Facebook Marketplace, or Instagram**

The scammer posts a fake advertisement.

They start a negotiation via WhatsApp, sometimes even sending (fake) documents.

Payment is requested via bank transfer or prepaid card top-up.

After receiving the money, they disappear.

- **3. Fake buyers**

If you are the one selling:

You receive messages from supposed buyers abroad who make up fees that must be paid in advance.

Or they ask you to go to the post office to collect the money, but force you to top up funds in their favor (Postamat scam).

How to recognize an online scam

- **Prices that are too low**
Offers far below the market price may be an attempt to quickly grab attention and push impulsive purchases without proper checks.
- **Request for upfront payment**
Scammers often ask for payment before delivery via bank transfer, prepaid card top-up, or other non-traceable methods, making it difficult to recover the money.
- **Unverifiable contact details**
The absence of a physical address, a real phone number, or reliable customer support may indicate an illegitimate seller.
- **Grammatical errors in messages**
Messages with obvious mistakes or machine translations can indicate scam attempts from unofficial sources.
- **Suspicious or unusual links**
Links with names similar to official websites or strange URLs may redirect to fake sites created to steal personal or banking information.

Real case: the social media scam

Tom, a 19-year-old student, finds a smartphone online at a very low price.

The seller asks for upfront payment via bank transfer.

After the payment, the seller disappears. Tom later discovers that the website had no verifiable contact details, the messages contained strange errors, and the link he received for shipping was fake.

👉 Tom never receives the product and also risks having his banking data stolen.

How to protect yourself from scams related to online buying and selling

Protecting yourself from scams is not impossible... you just need to follow a few simple but essential rules.

Pay attention to excessively low prices: they are the first warning sign of a possible scam.

When buying on auction sites (such as eBay), always check the seller's feedback.

Negative feedback = high risk of fraud.

Search the phone number or nickname on Google: it may have already been reported as a scam many times.

Do not trust identity documents sent by sellers or buyers:

They may be fake or stolen from other victims.

Never send copies of your personal documents to strangers:

They can use them to scam others or cause damage in your name.

If you are the seller, **never send money**: you are the one who should receive money, not the other way around!

Never go to a post office to receive a payment: you **cannot** receive money by inserting your card.

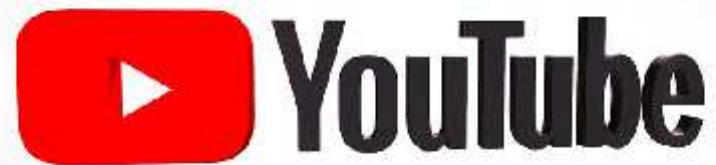
Anyone who asks you to do this is trying to scam you.

On e-commerce websites, always check that:

there are real contact details (phone number, email, address).

The absence of this information is a major red flag! Use only well-known websites with good reviews: if it's a clone or fake site, it usually has no reviews or only suspicious ones.

<https://www.youtube.com/watch?v=eMwqUqN8yUw>



How to avoid pitfalls when buying or selling online

When shopping online, the golden rule is: if something seems too good to be true, it probably is a scam. An item that costs significantly less than usual, such as a smartphone at half price, should immediately raise a red flag. Scammers use these “super discounts” to grab attention.

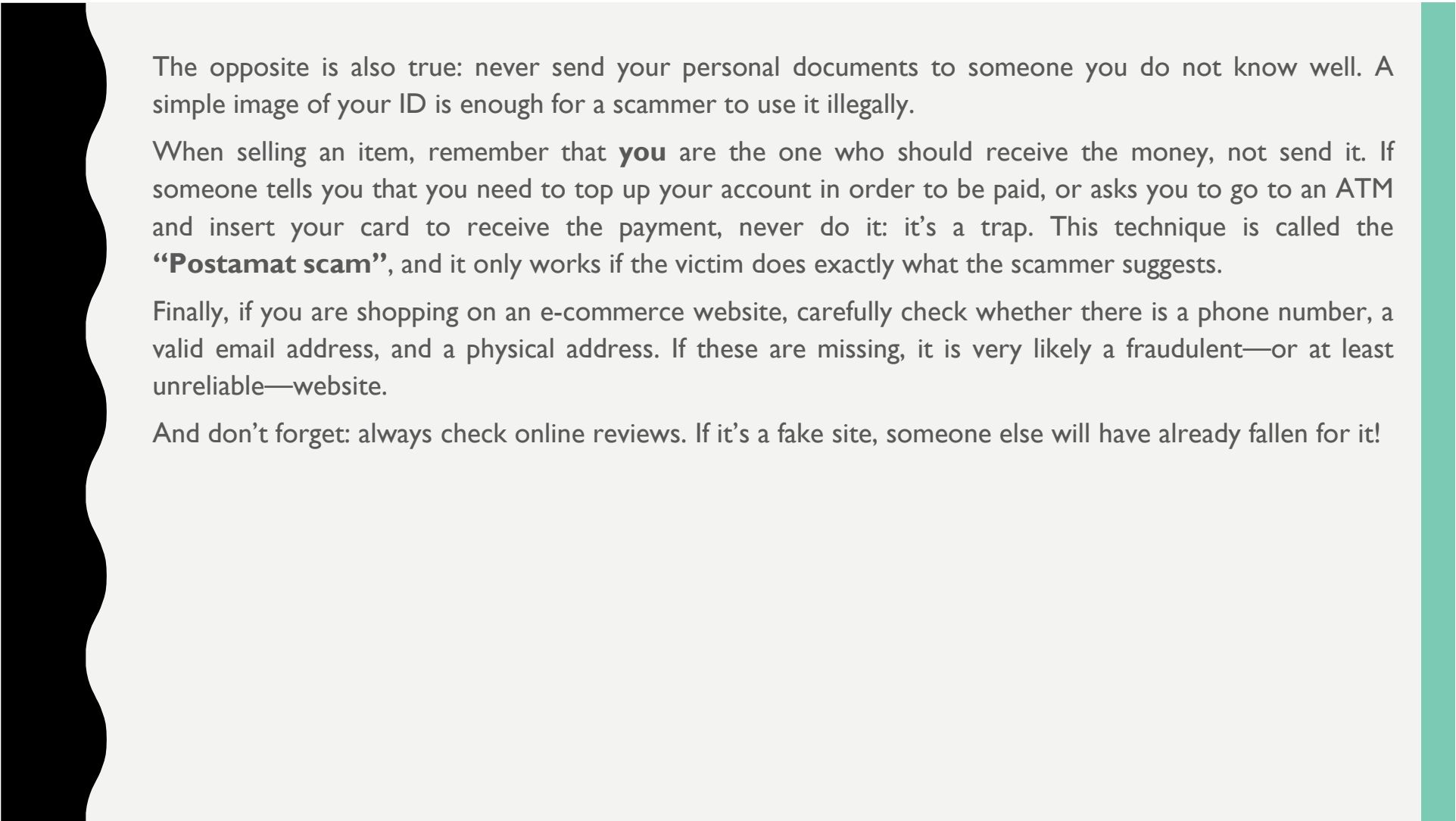
If you buy from an auction site or a platform such as eBay or Subito.it, always check the seller’s feedback. If they consistently receive negative comments or have a low rating, it’s best to walk away.

Another useful tip is to search the seller’s phone number or username on Google.

Other users often report scammers, and you may come across similar experiences.

And if someone sends you a photo of their ID to “prove” their reliability... be careful! That document could be fake or stolen from another victim.

Don’t trust something just because there’s a photo: everything you find online can be forged!



The opposite is also true: never send your personal documents to someone you do not know well. A simple image of your ID is enough for a scammer to use it illegally.

When selling an item, remember that **you** are the one who should receive the money, not send it. If someone tells you that you need to top up your account in order to be paid, or asks you to go to an ATM and insert your card to receive the payment, never do it: it's a trap. This technique is called the **“Postamat scam”**, and it only works if the victim does exactly what the scammer suggests.

Finally, if you are shopping on an e-commerce website, carefully check whether there is a phone number, a valid email address, and a physical address. If these are missing, it is very likely a fraudulent—or at least unreliable—website.

And don't forget: always check online reviews. If it's a fake site, someone else will have already fallen for it!

Watch out for the bait!

What is phishing and how are our data stolen?

Phishing is like fishing... except instead of catching fish, **we** are the ones being caught. Scammers cast a bait—usually a message that seems urgent or important—and hope someone bites by clicking on the link. These messages often appear to come from your bank, a delivery company, or even a well-known brand. They say things like:

“Warning, your account has been blocked!”

“You must confirm this transaction now!”

“There’s a problem with your package, click here!”

How to check if a link is safe

- **Always check the real domain of the website**
Make sure the web address is spelled correctly and matches the official site. Scammers often use names that look very similar to real ones.
- **Avoid shortened links or links with strange names**
Shortened links or those with unusual combinations of letters and numbers may hide fake websites.
- **Check the link before clicking**
Hover your mouse over the link (without clicking) to see the real address it leads to.
- **Do not enter personal data after opening links received via email or SMS**
If you receive a message asking you to log in or provide information, always go to the official website by typing the address directly into your browser.

What would you do?

You receive an online investment proposal promising easy and fast profits.

Possible choices:

- Invest immediately so you don't miss the opportunity
- Check whether the platform is registered or authorized in your country
- Talk to your bank or a financial advisor

👉 Which choice do you think is the safest?

⚠️ **How these scams work**

Scammers create urgency and anxiety to push you into acting without checking. They make you click on links that look official but lead to fake websites that steal login credentials and banking data.

Sometimes they even call you pretending to be your bank and ask for:

- OTP codes
- Card details
- Confirmations via app or fingerprint

👉 In this way, without realizing it, **you are the one authorizing the payment.**

⚠️ **No bank will ever ask for codes, PINs, or tell you to uninstall your banking app.**



How to protect yourself?

Never click on links in suspicious messages, even if they seem legitimate or appear to come from “Poste Italiane” or “your bank”.

If you receive a threatening or alarming phone call, hang up and call your bank directly using the official number.

Never give anyone your PIN, password, OTP, or CVV code. No bank will ever ask for them via SMS or phone.

If a message asks you to call back a number, first check that it is the bank’s official number. Even better, contact customer service directly yourself.

Remember: even if someone sounds polite, knowledgeable, and convincing... they could still be a scammer reading from a memorized script.

The online trading scam: the risk of losing everything

In recent years, especially after the pandemic, online advertising has increased, promising easy profits by investing in cryptocurrencies or shares of major companies such as Amazon or Tesla. These ads often appear on Facebook or Instagram and are accompanied by fake testimonials, exaggerated figures, and claims like: *“Start with just €250 and become rich in a week!”*

Behind these ads are fake financial advisors who call you from foreign numbers (often with the +44 prefix, indicating the UK) and speak in a convincing way, almost like real experts. They explain how trading works, make you feel special, and tell you that you could earn much more than with a traditional bank.

At first, they ask for only a small investment, such as €250. Then they give you access to a fake platform where you can see your money “growing.” Everything looks real. Within a few days, your initial investment appears to have doubled.

And this is where the real trap lies: they call you back and convince you to invest more. They tell you it's the right moment and that you'll earn even more. If you give in, you start transferring increasingly large amounts of money—thousands or even tens of thousands of euros.

To “help” you, they may ask you to install a program such as **AnyDesk** or something similar, which allows the scammer to remotely control your computer or phone. They will say it's just to assist you, but in reality they use it to transfer your money to anonymous accounts and wallets.

Finally, when you ask to withdraw your money, the problems begin: they tell you there has been a sudden loss and that more money is needed to “recover,” or they say you must pay taxes before you can withdraw.

And when they realize you won't send any more money... they disappear.



But it's not over: the second scam arrives

After being scammed, someone may contact you again pretending to be: a lawyer, a bank, or an authority that promises to help you recover the money you lost... but only after another payment.

You hope, you believe it, and you might even send money again. But it's just a second scam—one that is even more cruel than the first.



How to protect yourself?

Never trust anyone who calls you to propose online investments, especially if the number is foreign or unknown.

If you really want to invest, turn to a real bank or a financial advisor you can meet in person.

Always check on the ESMA website (European Securities and Markets Authority – www.esma.europa.eu) whether the company that contacted you is authorized to operate in the European Union.

Never install remote control software at the request of strangers.

Do not make transfers to foreign IBANs unless you are absolutely sure about the recipient.

And above all, don't be fooled by the illusion of easy money. Safe investments require time, patience, and expertise.

The broken or stolen phone scam

Imagine this: you receive a WhatsApp message from someone claiming to be your brother, cousin, or even your nephew, telling you that their phone is broken, they've changed their SIM card, and they can't make calls. Sounds strange, right? But wait—there's more!

To make it seem more realistic, the person even sends you very strange voice messages, filled only with annoying noises like *bzzzz* or *grgrgr*, making you think, "Wow, yes, the phone really is broken!"

Then comes the twist: they tell you they urgently need to make a payment—maybe to pay a bill, taxes, or a loan—but they can't because their phone is broken and they can't use online banking. So they ask you something like:

"Hey, can you do me a favor and make the payment for me? I'll give you my card details or IBAN..."

And you, trusting them, send the money.

Unfortunately, that's when you realize you've fallen straight into a scam!

But don't panic: the smartest thing to do is to pick up the phone (the real one!) and call your *real* relative—not the one who contacted you on WhatsApp. If they answer, bingo! You've uncovered the scam.

If they don't answer, don't panic and don't rush to do what the message asks. Take a moment, try calling another family member who might know what's going on (such as a daughter-in-law, son-in-law, or other relatives), and above all, **never** make a payment just because someone messaged you on WhatsApp.

And if you really want to be safe, you can also contact law enforcement and ask whether the situation sounds like a scam. Better safe than sorry!



The fake package scam

Okay guys, this scam happens especially during the holiday season, when we're all extremely busy shopping online. And guess what? You receive a message that looks like it's coming from a delivery company, saying something like: "Hey, there's a problem with your package!"

The message invites you to click on a link to fix the issue and finally receive your package. But be careful—it's a complete scam!

Here are some classic messages you might receive:

- *"Your package has been held at our shipping center. Follow the instructions here:" (with a link)*
- *"Hi, we were unable to deliver your package. Check here:" (with a link)*
- *"Your package may be delayed. Confirm delivery here:" (link)*
- *"Hi, your package is waiting for you to set your delivery preferences. Click here:" (link)*
- *"We have a package for you. To schedule delivery, click here:" (link)*

They look very official, right? But as soon as you click that link, you're taken to a page that looks exactly like the real courier's website—but it's a trap!

They ask you to pay something like €2 or a small fee to unlock the delivery. You enter your credit card details and... boom! They take those €2, but in the meantime you've unknowingly activated very expensive subscriptions to shady services, with monthly fees that can reach up to €50!

And trying to cancel those subscriptions? Almost impossible. The only thing you can do is report the fraud and block your card, requesting a new one.

A trick to avoid falling for it? Check the link carefully: if it doesn't start with **“https”** (the **“s”** is essential!), it means it doesn't have an SSL security certificate. Be very careful, because this is often a sign of a scam.

If you're expecting a package and you have the tracking code, go directly to the courier's official website and check where your parcel is. And if you have doubts, call the courier right away before clicking anything.

Rule number one: **never, ever, ever click on suspicious links!**



Identity theft

The problem is that social media profiles like WhatsApp, Instagram, and Facebook are the favorite targets of these scammers. And often—what’s even worse—someone uses our information to create fake profiles that look exactly like us!

How does social media account theft work? Often you receive a message from a contact (who has already been hacked) inviting you to click on a link. They might say something like “Take part in a survey” or something similar. But that link is a trap: it’s actually a confirmation link for a password change that someone is trying to make on your account. If you click it, you’re basically saying, “Yes, change my password!”—and the hacker gains control of your account.

Once inside, the hacker changes everything: password, email address, and even sets up two-factor authentication using their own phone number, locking you out completely. From there, they can use your profile to send strange messages to your friends, spread hate, boost influencers’ followers, and unfortunately even do really serious things, such as sharing illegal material.

What do you decide to do for your online safety?



What would you do in real life?

You receive an SMS: *“Your package is out for delivery. Click here to confirm your details or pay for shipping.”*

The message seems urgent.



Do you really have a delivery coming? What do you do?



Click the link immediately



Go to the courier's official website by typing the address into your browser



Contact customer service to verify the message



Which choice is the safest?

Some tips to avoid falling for it:

- Never click on suspicious links, even if they come from friends or relatives. If you have clicked, try to recover your account through official procedures, but it is often difficult.
- Do not post photos or content that reveal where you live, how you live, or excessively personal details. Also, pay attention to geolocation in photos!
- Never upload identity documents to websites or portals unless you are 100% sure they are truly necessary. Public authorities already have your data and will not ask you to upload anything.
- If a private individual asks for personal documents during a negotiation or a sale, refuse! It's a huge risk.

In short, with a bit of attention and common sense, you can feel much safer on the web!



Defamation and hate crimes

Attention, everyone!

Defamation is a serious crime that involves damaging someone's reputation or falsely attributing facts that harm them. With the rise of social media, this problem has grown dramatically because posts often spark heated discussions, and many people lose their temper, resorting to insults, slander, and attacks against those they disagree with.

When this happens on social media, it is even more serious, because the insults are seen by so many people—sometimes thousands. What we often call an “opinion” can actually amount to defamation, and those who suffer from it can file a legal complaint.

Added to this are the phenomena of haters—people who fuel arguments and hurl insults—and **hate speech**, meaning speech that incites violence or hatred against specific individuals or groups.

Italian law (Article 604-bis of the Penal Code) severely punishes incitement to hatred and discrimination, as well as propaganda based on race, ethnicity, religion, or other personal factors.

In addition, there is a recommendation by the **European Commission against Racism and Intolerance (ECRI)** of the Council of Europe (Recommendation No. 15/2015), which explains what hate speech is: all forms of communication that promote or incite denigration, hatred, stigmatization, or threats against a person or group based on reasons such as race, color, origin, religion, gender, sexual orientation, and others.

When we take part in online discussions, we should always remember to use good manners and common sense, just as we do in real life.

Unfortunately, the anonymity of the internet and the feeling of distance from others often bring out the worst in us, leading us to behave like trolls or haters without even realizing it. This phenomenon is known as the “**Gyges effect**” (from the myth of Gyges told by Plato), when we feel untouchable simply because we are online.

So let's always respect others, use the internet responsibly, and not allow anonymity to turn us into bad people.

The web is a serious place too, and the rules of civility and the law apply there as well.



The internet is a powerful tool: it can inform, connect, entertain...

But it can also deceive you, steal your data, spread hate, or scam you in just a few seconds.

Knowing how to recognize online dangers isn't paranoia—it's intelligence.

Don't click randomly. Don't trust something just because it "looks real." Never underestimate the consequences.

As Ed Sheeran said:

"Give me a little time..."

Well—before you click, take a moment.

Think. Check. Ask.

Because online, those who stop (to think) stay safe.





cre thi dev
creative thinking development



Co-funded by
the European Union

Funded by the European Union. The views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Innovation Council and the Executive Agency for SMEs (EISMEA). Neither the European Union nor EISMEA can be held responsible for them.