Digital Security: Protect Yourself from Fraud and Scams
Too good to be true?

Stay safe and secure protect yourself from deception.
Learn how to spot someone pretending to be your bank.
If you've received a suspicious message or believe you've been a victim of fraud, contact your branch or the Digital **Branch immediately.**

Do you think you've been the victim of online banking fraud or an attempted scam?
If you have any doubts about a communication, the best thing to do is to call your branch or the Digital Branch.
Online banking fraud is becoming increasingly deceptive

Phishing and its shades

For a happy ending, be cautious of anyone pretending to be someone else through **emails, messages, or phone calls.**

Find out more – Is it really your Bank calling you?

Your smartphone is getting smarter and often alerts you when you're receiving a spam or marketing call. But if the call comes from an Intesa Sanpaolo number, can you always trust it?
The answer is no. Many fraud attempts today involve calling customers directly from official-looking numbers, such as the toll-free number **800 303 303** of the Online Branch.

Here are **4 important things to remember:**

The Digital Branch number can only receive calls, it cannot make them.
If you receive a call from this number (**800.303.303** for individuals, **800.312.316** for businesses), it is definitely a fraud attempt.

The Bank will never ask for your login or security codes. If you receive a call asking for your internet banking credentials or security codes to authorize transactions, it's not us calling you.

Every request may sound convincing, but that doesn't mean it's trustworthy. Even if the caller sounds legitimate, if they ask for your internet banking or app credentials, tell you to download an app, or visit a link they are trying to deceive you.

Never download apps or click on links requested via phone call, SMS, or email.
There's a risk that these apps may contain viruses or malware capable of taking control of your device and stealing your personal and confidential information, such as your banking login and security codes.

Is it really your Bank messaging you?

Every day you receive countless communications via email and SMS, some of them may look authentic, but aren't.
In particular, an SMS might even appear within the genuine message thread from your Bank, thanks to sophisticated techniques used by cybercriminals.

Digital Security: Protect Yourself from Fraud and Scams
Too good to be true?

The Online Investment Scam

Always be wary of anyone offering easy profits. Don’t be fooled by online investment scams.

Find out more – How does it work?

You receive a phone call; a recorded voice offers you investment opportunities with high returns, often using the names of well-known companies.

- The call is then **transferred to a fake financial advisor** who, using social engineering techniques, tries to convince you to sign up for a fake trading platform often assisting you through the process using screen-sharing tools.
- **The scammer**, **pretending to be a financial advisor**, encourages you to make a small initial deposit via bank transfer or credit card payment.
- In the following days, the scammer shows you **fake data on the fraudulent trading platform**, displaying supposed profits from your initial investment to persuade you to deposit more funds.
- At this point, if you try to withdraw the funds you believe you've earned, the scammer tells you that you need to make another deposit either to reach a withdrawal threshold or to pay taxes. **No funds are ever returned, and you realize you've been scammed.**

Learn to recognize the signs and protect yourself

Verify the reliability of the trading platform you’re using

Don’t be fooled by promises of **easy money**

Be suspicious of messages containing **unknown links or phone numbers**

Digital Security: Protect Yourself from Fraud and Scams
Too good to be true?

The Romance Scam

The frog doesn’t always turn into a prince. Don’t be charmed by online romance scams.

Find out more – What are the warning signs?

Scammers may target you not only on online dating sites, but also through social media or email.

- Someone you've recently met online **claims to have strong feelings for you** and asks to chat privately.
- **Their messages are often vague**, may contain spelling or grammar mistakes, and they might ask you to send personal photos or videos. Also, their online profile doesn’t match what they say.
- After gaining your trust, the person **asks for money, gifts, or your credit card** or bank account details.
- If you refuse to send money, the scammer may try to **blackmail you.** If you do send money, they’ll keep **asking for more.**

What can you do?

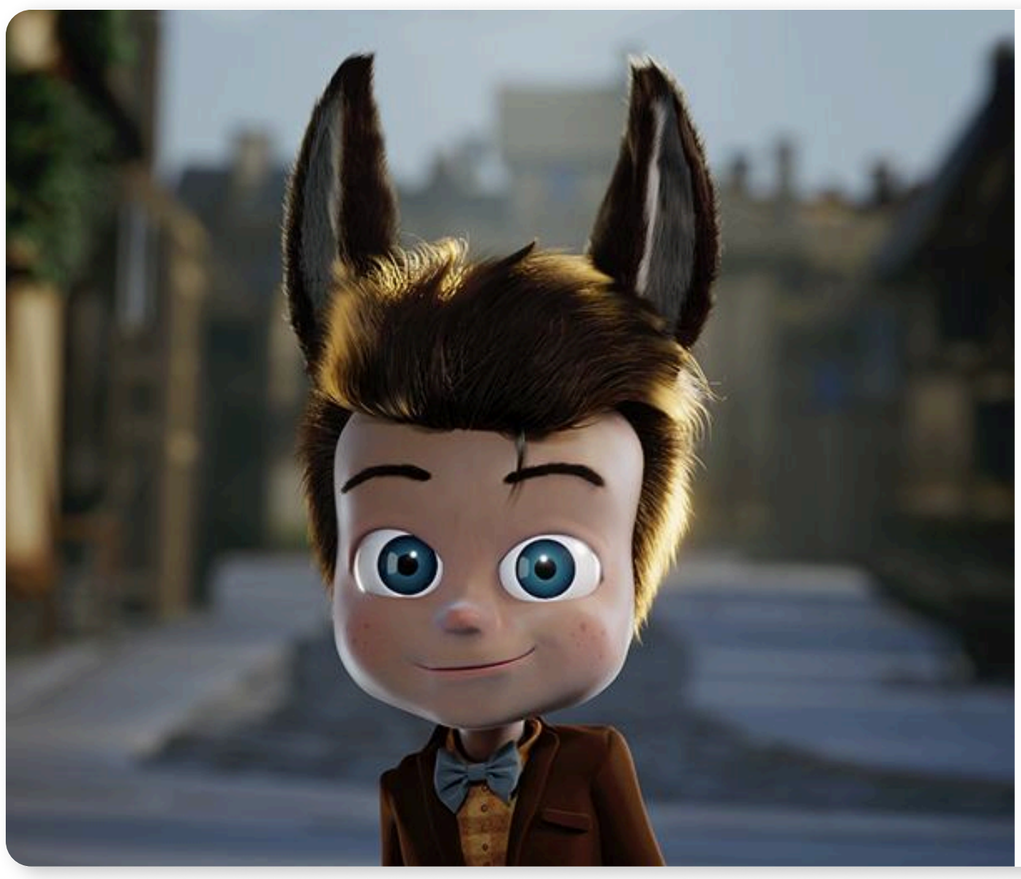
- Be very cautious about the personal information you share on social media and dating sites
- Always consider the risks, scammers are present even on trusted platforms
- Be careful and ask your contact more details
- Do a reverse image search of their photos and profile to see if they’ve been used elsewhere
- Watch for spelling and grammar errors, inconsistencies in their stories, and excuses (like a broken camera)
- Never share compromising material that could be used for extortion
- If you agree to meet in person, tell family or friends where you're going
- **Never send money, share credit card or account details, or copies of personal documents**
- Avoid making upfront payments
- Never transfer money on someone else’s behalf, money laundering is a criminal offense

Has it happened to you?

Don’t feel ashamed!
Break off all contact immediately and, if possible:

1. **Save all communications,** such as chat messages
2. **Report** it to the competent Authorities
3. **Report the scam** to the website through which the scammer first contacted you
4. If you shared your bank details, **contact your Bank** immediately

Digital Security: Protect Yourself from Fraud and Scams
Too good to be true?



The Money Muling Scam

Be careful with bad company, you could become an accomplice of money muling.

Find out more – How does it work?

Not just a victim: with this scam, you could unknowingly become an accomplice in money laundering as a “money mule”
(a courier who moves dirty money through their own bank account).

The scammer contacts you by phone from foreign numbers or through instant messaging apps; they offer you a job promising easy earnings in exchange for liking social media pages or posting positive reviews on platforms.

To make the offer more convincing, they **add you to a WhatsApp or Telegram** group where you’re asked to leave likes or write reviews in exchange for small payments (€20-40).

In some cases, you’re also offered the chance to **earn much more if you transfer money** to the scammer’s account. Thinking it’s a safe profit, you end up sending increasing amounts of money to the scammer.

The scammer may also propose easy money by asking you to:

- **Use your bank account** to transfer money provided by the scammer to a third party;
- **Open a new bank account** and hand over its management to them;
- **Send them photos of your ID documents**, so they can open bank accounts in your name without your knowledge.
- In all these cases, you could unknowingly **become an accomplice to a financial crime.** Always stay alert and don’t trust anyone promising easy money!

What to do and what not to do

- ✗ Never open a bank account at the request of someone you’ve just met
- ✗ Don’t allow your bank account to be used on behalf of others
- ✗ Don’t make bank transfers or send money to strangers, even if you are promised compensation
- ✗ Never share your banking details with anyone unless they are people you know and trust
- ✗ Don’t be fooled by spontaneous offers of easy money: if it sounds too good to be true, it probably is
- ✓ If you receive a job offer, research the company using accredited and recommended websites
- ✗ Avoid joining unknown Telegram or WhatsApp groups; if you are added by someone, leave immediately and report it
- ✓ Be cautious of unknown phone numbers (especially foreign ones) and check online if these numbers or email addresses are linked to scams
- ✓ If you believe you are involved in this scam, stop all money transfers immediately, notify your bank, and report it to the competent Authorities

INTESA SANPAOLO

Digital Security: Protect Yourself from Fraud and Scams
Too good to be true?

Discover more examples of frauds and scams

Fake websites

Fake messages may contain a link to a counterfeit website that at first glance looks identical to the bank's official site.

Find out more
How can you recognize a fake website?

The address bar shows a "not secure" label

The website's domain is incorrect

There are typos in the website address

Phishing

To recognize a phishing email, it's important to pay attention to certain elements in the design and text.

Find out more
How can you recognize a phishing attempt by email?

The sender's email address is not official

You are asked to confirm your credentials online

The email text may contain typos, grammatical, or spelling errors

You are given an "ultimatum" to perform a specific action

Any links (for example, to the Bank's website) are not official

Family Emergency Scam

How the scam carried out by a "fake" relative works.

- The scammer sends you an SMS **pretending to be a relative** or friend in an emergency situation and asks you to contact them on a different phone number than usual.
- If you continue the conversation (often via an instant messaging app or social network), the scammer —after some casual messages—asks you to make **urgent payments**, such as bank transfers or Western Union, to resolve the emergency.
- If you make the requested payments, thinking you're helping a relative or friend in trouble, the **funds are actually transferred** to the scammer.

Find out more
Learn to recognize the signs and protect yourself

Pay attention to messages containing unknown links or phone numbers

Pay attention to urgent requests

End the call and contact the Bank or a trusted person for help

Fake agent Scam

How the scam of saving financial funds in danger works.

- You receive an **SMS, apparently from the Bank**, containing a link to a website that looks like the original internet banking site but is used by the scammer to steal your banking credentials and other personal data.
- The scammer calls you, **pretending to be an anti-fraud agent** from the Bank and/or Postal Police to gain your trust. They alert you about false "fraudulent transactions temporarily blocked" on your account.
- At this point, the scammer tries to convince you to urgently go to a **branch to "secure" your funds** by making payment transactions (usually instant bank transfers) to a new bank account.
- If you go to the branch, the scammer persuades you over the phone to make a **transfer to a new fraudulent IBAN** they provide. Believing you are "securing your savings," you instead transfer the money into their account.

Find out more
Learn to recognize the signs and protect yourself

Pay attention to messages containing unknown links or phone numbers

Pay attention to urgent requests

End the call and contact the Bank or a trusted person for help