Faculty of
Finance and Banking

Safety in the digital world



Preventing online fraud, keeping card transactions secure, protecting personal banking data

Institutional project

Improving financial knowledge and skills among young people in Romania

2026

Table of contents

1. Defining online financial fraud ---------- **3**

2. Official classifications of online financial fraud ---------- **4**

3. Common types of fraud in Romania ---------- **5**

3.1. Phishing 6

3.2. Investment Scams 8

3.3. Spoofing 11

3.3. Deepfakes 13

3.3. Online Shopping Platforms Fraud 14

4. How to spot and avoid common online scams and fraud ---------- **15**

References ---------- **22**

Disclaimer: In an increasingly challenging online environment, where cyber threats are constantly evolving, knowing how to recognise and prevent fraud is the most important step in protecting your savings. This guide gives you the essential knowledge to build effective digital protection. Responsible money management always starts with keeping your money safe. The Faculty of Finance and Banking urges you to stay alert and to report any suspicious attempt without delay. Always check official channels before providing confidential information or opening unusual links. Since recommendations may be updated over time, we suggest you check official information regularly.

1. Defining online financial fraud

Online financial fraud covers all intentional actions in which criminals use technology, communication networks and digital infrastructure to deceive victims, in order to obtain illicit profits or cause financial damage to individuals and companies. This crime is hybrid in nature: it combines technical methods (exploiting security flaws in software or hardware, intercepting data and manipulating systems) with social engineering, which exploits users' trust, inattention or lack of knowledge.

In general, online financial fraud rests on three main pillars:

1. **The technological channel:** internet and telephone networks, banking platforms, e-commerce websites, mobile apps and the devices used (phones, PCs, tablets).
2. **The economic target:** money, cryptocurrencies, confidential banking data (cards, PIN codes, passwords, authentication codes) and electronic means of payment.
3. **The attack mechanism:** methods such as phishing, malware, account takeover, transaction forgery or taking remote control of devices.

The defining feature of these frauds is that criminal activity has moved into virtual space. Because attackers are no longer limited by a physical location and can act from anywhere in the world, identifying them and holding them accountable becomes difficult. Moreover, their cross-border nature often goes beyond the scope of national legislation, making international cooperation crucial for prevention and investigation.

Legally, these acts fall under both cybercrime and economic and financial crime. They are regulated by national legislation (the Criminal Code, Law 161/2003) and by European directives and international treaties (Directive (EU) 2013/40, Directive (EU) 2019/713, the Budapest Convention). Their impact is twofold: on the one hand, they cause direct financial losses to victims; on the other, they weaken public trust in digital payments, affecting economic stability and cybersecurity in the long term.

2. Official classifications of online financial fraud

A comparative analysis shows that national typologies tend to be more pragmatic and closely aligned with local realities, focusing on the threats most common in a given socio-economic environment. European typologies, by contrast, take a broader view that includes complex scenarios and phenomena with significant geopolitical dimensions.

Bringing these two distinct but complementary perspectives into a single analytical framework not only makes the classification of online financial fraud more accurate, but also strengthens cross-border cooperation in fighting these insidious crimes. By aligning their efforts and sharing information, nations can be better prepared to deal with the increasingly sophisticated nature of online financial fraud and the challenges of its transnational operations.

By method (technical criterion)

- **Phishing –** sending deceptive e-mails or messages that appear to come from banks or payment platforms, in order to collect banking data.
- **Vishing and smishing –** obtaining confidential information through fraudulent phone calls or SMS messages.
- **Pharming –** redirecting users to fake websites by compromising DNS servers.
- •Financial malware – banking trojans, keyloggers, ransomware that also steals financial data.
- **Business Email Compromise (BEC) –** intercepting and falsifying business correspondence in order to divert payments.



By purpose

- **Obtaining funds directly –** unauthorised transfers from the victim's accounts.
- **Obtaining funds indirectly –** reselling financial data on illegal markets.
- **Facilitating money laundering –** successive transactions through fintech platforms or cryptocurrencies.

By type of victim

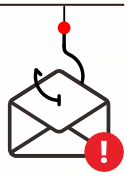
- **B2B fraud –** attacks on companies' payment and invoicing infrastructure.
- **B2C fraud –** deceiving consumers through fake online shopping platforms**.**
- **C2C fraud –** deceptive listings on marketplace platforms.

3. Common types of fraud in Romania

Today, cyber fraud has gone beyond isolated incidents and become a complex phenomenon, backed by well-organised global criminal networks. These specialised groups use an advanced mix of technical tools and psychological tactics to carry out their attacks.

Criminals combine exploiting weaknesses in systems — such as software bugs, weak passwords or insecure connections — with social engineering. This two-pronged method allows them to manipulate human behaviour, leading victims to unwittingly hand over confidential data or take actions that compromise their security. Moreover, attackers adapt quickly to new technologies and changes in user behaviour, making fraud increasingly difficult to detect and prevent.

Understanding these mechanisms is an essential step towards creating effective protective measures and strengthening digital security, both for individuals and for organisations.



3.1. Phishing

Phishing is a form of computer fraud based on sending electronic communications (e-mail, SMS, in-app messages) that imitate legitimate sources, in order to obtain sensitive data (passwords, PIN codes, bank card details, personal information). In essence, this type of attack combines social engineering with technological exploitation to compromise the security of the victim's financial data.

Whatever the scenario, phishing attacks usually follow the same structure:

- Creating a false identity – impersonating a bank or financial institution;
- Sending the fraudulent message – through electronic channels;
- Creating a sense of urgency or fear – to prompt quick, unquestioning action;
- Redirecting the victim to an environment controlled by the attacker – a cloned website or fake form;
- Collecting the data – storing the credentials in illicit databases;
- Exploiting the data – fraudulent transactions, selling on the dark web, taking out loans.

Real-life scenarios

A. Links sent in the bank's name to “update your banking details”

Techniques and tools used:

- **Sender forgery (e-mail spoofing):** The attacker disguises the real address by changing the “From” field. Even if a legitimate name appears at first glance (e.g., Your Bank suport@banca.ro), checking the technical header will reveal the real sender, such as server123@hosting-dubios.com.
- **Phishing kits (cloning packages):** These are ready-made (“turnkey”) websites. Criminals download archives of web pages that perfectly imitate the bank's pages. The only difference is that the login form sends the data entered directly to the attacker (by e-mail or to a private database) instead of logging you into your account.

- **Misleading security certificates (SSL/TLS):** The “padlock” in the address bar only indicates an encrypted connection, not that the website can be trusted. Attackers easily generate free certificates (e.g., Let's Encrypt) for their cloned sites, creating a false sense of security.

- **Psychological manipulation:** This relies on creating urgency and invoking authority. Messages such as “Your account will be blocked within 24 hours if you do not reconfirm your details” are deliberately designed to trigger panic, so that the victim acts quickly without checking the details.

B. Message informing the victim of a card payment and asking them to confirm

Techniques and tools used:

- **The emotional trigger of panic:** Alarming phrases are used, such as “Suspicious transaction detected”. The messages leave no breathing room — they use words like “Now”, “Immediately” or “Pending” to block the victim's analytical thinking.

- **Trap text messages (smishing):** Shortened links sent by SMS that redirect to phishing pages designed specifically for mobile devices.

- **Simulated mobile interfaces:** Cloned web pages that imitate official banking apps down to the pixel to trick the user.

- **Redirect servers:** Technical infrastructure used by attackers to hide their real identity and location.

- **The psychological mechanism behind it:** Creating an artificial sense of urgency, which leads the victim to react impulsively and skip security checks.

Message type	Example text (simulated)	Tactic analysis
Banking urgency	"INFO [Your Bank]: A payment of 2,450 RON to 'eMAG' is pending. If you did not authorise this transaction, cancel it here: https://bit.ly/check-secure-ro"	Uses the name of a well-known bank and a large amount to cause immediate panic.
Account security	"Security Alert: A new device has logged in to your account from Moscow. If this wasn't you, secure your account now: https://banca-suport.net/login"	Combines fear of unauthorised access with suspicious geographical locations.
Card verification	"[CardControl]: Your card has been temporarily blocked for security reasons. To unblock it, confirm the last 4 digits here: https://verificare-card.com"	Creates a major inconvenience (a blocked card) to force the user to click.

3.2. Investment Scams

Investment scams involve manipulating victims into directing capital towards non-existent financial opportunities, falsely presented as offering high returns and low risk. The end goal is to divert the funds into the attackers' accounts. Operationally, the scheme relies on aggressive online promotion and on remote access software used to take control of devices. Investment scams show a sophisticated combination of online marketing technologies, remote control tools and direct exploitation of the victim's personal banking infrastructure. This hybrid technical and psychological approach considerably increases the success rate of the attacks.

The typical stages are:

A. Identifying and luring the victim

- Paid ads on social media (Facebook, Instagram, LinkedIn, TikTok): Ads optimised through advanced targeting (microtargeting) to reach users interested in areas such as investing or financial education.
- Cloned landing pages: Websites that faithfully copy the look of real trading platforms or trusted financial portals.
- Fake reviews and testimonials: Fabricated texts, images or videos (featuring supposed "successful investors") used to create a false impression of legitimacy and safety.

B. Direct contact with the victim

- Calls from fake agents (boiler rooms): Phone calls from trained operators who use well-rehearsed scripts to gain the victim's trust quickly.
- Caller ID spoofing: A technique in which attackers disguise the caller's identity, so that the phone screen shows the number of a bank or a legitimate authority.
- Persuasion and psychological manipulation: The criminals present themselves as "financial advisers" or "investment experts", using manipulation tactics based on authority, urgency and simulated personal attention.



How to spot a "boiler room agent"

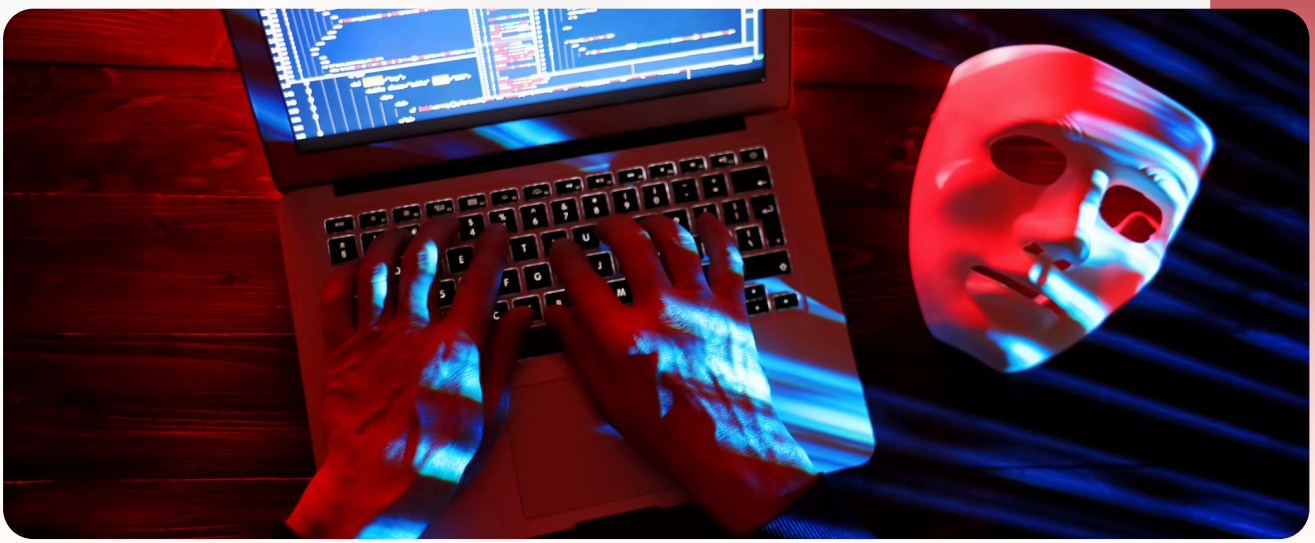
- Guaranteed profit: "There is no risk, losing money is impossible." (In reality, every investment carries risk.)
- Isolating the victim: "Don't tell anyone about this offer, it's confidential/only for VIP clients."
- Time pressure: "We have to decide now, otherwise the price goes up."
- Installing software: Being asked to install remote control programs (AnyDesk, TeamViewer).

C. Being asked to install remote control apps

- Misuse of legitimate remote control apps: Official programs such as AnyDesk, TeamViewer or RemotePC are falsely presented to the victim as “technical support” tools for setting up the investment.
- Manipulation to gain full access: Social engineering techniques that lead the victim to grant extensive permissions on the device (control of the screen, keyboard, files and notifications).
- Hiding the real intentions: Attackers justify installing the apps by claiming it is a mandatory step “to guide you step by step” in opening a trading account.

Clear warning signs (red flags)

- Any request to install AnyDesk, TeamViewer or RustDesk from someone you don't know (however polite or professional they sound).
- Being asked to log in to your banking app while a remote control session is active.
- Pressure to grant “Accessibility” or “Screen Recording” permissions on your phone.



3.3. Spoofing

Spoofing is the deliberate falsification of the identifying attributes of a communication channel (IP, e-mail address, phone number) to imitate a trusted source. In banking fraud, caller ID spoofing is used to display the official contact number of a financial or public institution, in order to extract sensitive data or get illicit transactions authorised.

A. Obtaining and using caller ID spoofing technologies

- Internet telephony (VoIP) services with an identity-changing option: Platforms often operated from countries with permissive legislation, which allow the number displayed on the recipient's screen (Caller ID) to be changed.
- Dedicated call-spoofing tools: Specialised platforms and apps (spoofing tools) through which attackers can manually enter any phone number they want to appear on the victim's screen.
- Illegal takeover of the phone number (SIM swap): In more advanced scenarios, criminals manage to fraudulently port or transfer the victim's real number to another SIM card, thereby taking control of the victim's calls and messages.

B. Impersonating trusted institutions

1. Impersonating a bank's call centre

- Faking the official number: The attacker calls from the bank's real number and claims that the victim's login details have been compromised, asking for them to be “validated” urgently.
- Complex conversation scripts: Well-prepared scenarios in which attackers mention the customer's real data (obtained earlier from data leaks) to remove any suspicion.

2. Impersonating the National Bank of Romania (BNR)

- The pretext of financial countermeasures: The caller claims to represent the BNR and to be trying to “protect” the victim by blocking a supposedly illegal loan taken out in their name.
- The false authority tactic: Attackers introduce themselves using the names of real BNR employees and cite fictitious laws or regulations to appear fully legitimate.

3. Impersonating the Police

- Invoking a criminal investigation: The call appears to come from an official police station. The victim is told that their data has been stolen and is asked to urgently withdraw their money (including through quick loans) and deposit it in a Bitcoin ATM “for safety”.
- Psychological pressure and emotional blackmail: Creating extreme urgency under the pretext of helping with a secret investigation, with a strict deadline for carrying out the instructions.

Immediate defence strategies

The “Hang up and call back” rule: If you get a call from the “Bank” or the “Police” asking for data or transfers, hang up immediately. Look up their official number on their website and call them yourself. Spoofing only works on incoming calls, not on calls you make.

Identity check: No institution (BNR, Police, Bank) will ever ask you over the phone for: your PIN or codes received by SMS; to install apps (AnyDesk); to transfer money to “safe accounts”.

SIM swap protection: If your phone suddenly loses signal (showing “No Service” or “Emergency calls only”) for no clear reason, immediately contact your mobile operator from another phone and check whether a number port or SIM replacement has been requested.



3.4. Deepfakes

Deepfake fraud involves using generative artificial intelligence and neural networks to create or alter images, video clips or audio recordings that are extremely realistic but completely fake. In finance, criminals use deepfake technology to impersonate public figures, institutions or trusted brands, lending false legitimacy to fictitious investment schemes designed to attract money.

1. Exploiting the image of public figures (politicians, economists, entrepreneurs)

- **Fabricated investment endorsements:** Creating video or photo material in which a public figure appears to be promoting high-return financial opportunities. This is done through:
  - Face-swapping and lip-syncing: Technologies based on generative AI models (e.g., DeepFaceLab, FaceSwap) that transfer facial expressions onto another body.
  - Voice cloning: Software such as ElevenLabs or Respeecher, used to synthesise and faithfully imitate the real person's voice and intonation.
- **Manipulation through authority:** Attackers use the reputation and fame of a public figure to falsely guarantee that the investment is safe.

2. Misusing the name and identity of public institutions

- **Counterfeit official announcements:** Generating deepfake videos in which real or fictitious representatives of ministries or state agencies announce “exclusive” opportunities to buy shares, through:
  - Combined video generation: Overlaying a synthesised face and voice onto an actor reading a scam script.
  - Authentic visual and graphic elements: Using logos, visual identity and original graphic elements taken directly from official websites to deceive the viewer.

3.5. Online Shopping Platform Fraud

Online shopping platform fraud covers all illegal practices carried out on e-commerce websites, classified-ad platforms or social media, in which buyers or sellers are deceived into handing over money. In general, this scheme exploits trust in online payments and transactions, creating the illusion of a completely legitimate sale or purchase.

As to how the fraud works, the criminal posts extremely attractive listings, with prices well below market level, to rush the buying decision. Once they receive the money (in full or as a deposit), they cut off all contact and never send the product.

Commonly used techniques include:

- Fake profiles or accounts created on popular platforms (such as OLX, eMAG Marketplace or eBay).
- Images and descriptions copied directly from other sellers' genuine listings.
- Hard-to-trace communication channels, such as temporary e-mail addresses and virtual (VoIP) phone numbers.



What to do if you have already entered your card details?

- Block your card immediately in your banking app.
- Contact your bank to report the fraud and request a new card.
- File a complaint with the Police (you can also do this online on the Romanian Police portal), providing evidence: screenshots of the conversation, the fraudulent link and proof of the transaction.

4. How to spot and avoid common online scams and fraud

Fortunately, you can protect your personal information by taking a proactive approach to cybersecurity. Vigilance protects you from cybercrime, but you should be ready to act quickly if your information is stolen. We are here to help — our comprehensive guide to personal cybersecurity can prepare you to protect yourself against scams and fraud, or to recover from them.

Account hijacking

Account hijacking means that an identity thief obtains your login details for a social media, e-mail or online banking account. Among other possible consequences, the attacker could use the stolen account to make the victim look bad, to steal their money, or to pose as the victim in order to deceive another person whose account is worth more.

The last decade has seen high-profile data breaches:
• In 2023, T-Mobile suffered two data breaches that affected 37 million customers.
• From 2019 to 2023, Facebook exposed more than 540 million user records.

In other words, it is very likely that some of your personal information has already been exposed. It is important to take precautions to prevent someone from obtaining enough additional information to access your accounts.

How to spot it?

- Someone you know contacts you with an offer that is “too good to be true”.
- Someone you know contacts you from a strange phone number.
- Someone you know starts posting strange offers on social media.

How to avoid it?

- Update your passwords regularly, use two-factor authentication (2FA) and protect your web traffic with a virtual private network (VPN). Also make sure that all your passwords — or, even better, your passphrases — are unique to each of your accounts. Automation has made it easy for criminals to test login details across different websites, so if you reuse passwords, once one account is compromised, the others could be too.
- If you suspect that one of your accounts has been accessed without your permission, contact your bank's customer support department immediately.

Impersonation scams

A fraudster pretends to be someone you know, a government representative or an employee of a company you might do business with. They want to manipulate you into sending money or sharing personal information. They may fake phone numbers or e-mail addresses to appear legitimate. They might try to take control of your computer by sending a malicious link, or ask you to send them money by gift card or bank transfer, which is like handing cash to the fraudster; if you fall victim to such a scam, you will most likely not get your money back.

How to spot it?

- They claim to be from technical support and call you about a problem with your computer.
- You have to pay them or click on a link they send you.
- They claim you owe money to ANAF (the Romanian tax authority).
- You have just won a prize in a competition you don't remember entering, but you have to pay fees to receive it.
- A friend is in trouble and needs your help.
- You have received a bank transfer for too large an amount and you need to send back the difference (a refund).

How to avoid it?

- Don't send gift cards or bank transfers to people you don't know.
- Never send money without first checking who contacted you, even if you think you know the person or they claim to be a friend or relative.
- Don't give personal information to people you don't know.
- Don't give people you don't know access to your computer.

The “sweetheart” scam

A “sweetheart” scam is a trick in which a fraudster uses emotional manipulation to win the target's trust. Using online dating apps and similar tools, the fraudster persuades the target to send money or share personal information.

Also be wary of the variant known as “pig butchering”. It usually starts with a text message presented as an accidental contact to a wrong number or an attempt to reconnect with an old friend. The fraudsters try to keep the target talking in order to build a relationship (a process called “fattening the pig”) before introducing the prospect of a lucrative investment opportunity, often in cryptocurrencies.

How to spot it?

- An online acquaintance declares strong feelings for you, even though you have never met.
- Someone you met online asks for a cheque, a postal order or a bank transfer.
- Someone contacts you through a dating site but claims to live in another city or country.
- A stranger needs urgent help and/or offers a financial incentive.

How to avoid it?

- Be extremely cautious about requests from someone you have never met, especially if you have no mutual connections. These fraudsters take advantage of our desire to be valued and our willingness to help — it is an extremely effective scam and calls for a high level of vigilance.
- Never send money to a stranger you met online.
- Recognise that “sweetheart” fraudsters will try to manipulate you emotionally.
- They will claim to have fallen in love with you, and then ask for money for a cause that plays on your sympathy.
- Their aim is to get as much money from you as possible, either gradually or all at once.

Phishing, vishing, smishing, quishing

Phishing is a form of social engineering in which fraudsters use e-mail to impersonate a business or a trusted person, in order to trick or intimidate people into giving sensitive information, sending money or downloading malware. Phishing messages are often sent to large numbers of people at the same time. A more targeted variant is called “spear phishing”, in which fraudsters use social engineering and spoofed messages to target one or more individuals in a specific organisation. For example, they might fake a message from the target's employer, asking them to provide critical information or make a financial transaction that bypasses normal procedures.

When a fraudster uses phone calls, the process is known as voice phishing or “vishing”. Similarly, “smishing” tactics use SMS messages, and “quishing” uses QR codes that lead to fake websites or malware. In all its forms, phishing imitates communications from brands, companies and people you trust.

How to avoid it?

The aim is to persuade you to give up your personal or confidential information by creating a false sense of urgency or desire. These fraudsters often use fear, false authority or other emotional manipulation to make you lower your guard. If you have doubts about a message:

- Never trust a request for your password — your password is for you alone. A legitimate source will not need your password, PIN or debit/credit card number to access your account information.
- Call the organisation directly; don't open any link in the message.
- Look up information about the company that sent the communication.
- Report the incident to the National Cyber Security Directorate (DNSC).

Quick money, unexpected winnings and offers “too good to be true”

These messages promise unexpected money, often in exchange for a fee or a tax. The best-known version involves a prince in crisis who asks for help transferring funds out of his country. However, fraudsters may also claim to represent cash-prize competitions, rebate programmes or the inheritance of wealthy relatives. The aim is to lure you into handing over money or personal information.

Some modern versions involve listings on online marketplaces such as Facebook Marketplace:

- A seller offers items at a price far below their real value.
- A potential buyer offers to pay more in exchange for a promise that the difference will be refunded.
- A rental listing in which the “landlord” insists on a bank transfer for the deposit before meeting you or letting you view the property.

How to spot it?

- Someone offers you money unexpectedly.
- You receive a message from someone you know, but from an unknown e-mail address or phone number.
- Someone asks you to deposit a cheque on their behalf and offers you part of the cash.
- An online listing states that the “landlord” doesn't want to meet first and asks for a deposit.
- An online seller wants to “verify” your identity with a code sent via Google Voice.

How to avoid it?

You should always be suspicious if a lawyer, a bank or a company contacts you offering any sum of money — even if the offer includes documents that look official. If you are contacted, don't send money and don't try to deposit unverified funds, especially if you have never met the sender. A cheque could be fake, and a transfer through a payment app could turn out to be fraudulent. Your financial institution may make the funds available at first, but if the deposit is later reversed and the money is taken back from your account, you will lose whatever part of that deposit you have withdrawn or spent. Ask a lawyer or financial adviser for advice if you have suspicions about a communication.

Fake approval messages

A common example of this scam is when attackers send fake approval notifications to consumers, claiming that the target has been “pre-approved” for a line of credit, a mortgage or a personal loan. The aim is to persuade the target to provide personal information or financial account details in order to accept the offer.

Recent university graduates are often targeted with fraudulent credit card offers. Home buyers are vulnerable to real estate scams. Similarly, attackers may pose as insurance companies offering federal tax exemptions after a natural disaster. Impersonation scams are the most frequent complaint made to the National Cyber Security Directorate (DNSC).

How to spot it?

- You are approved for an offer you don't remember applying for.
- You are offered insurance compensation for a policy you don't hold.

How to avoid it?

Always be cautious about lenders who:

- Promise to negotiate a change to your loan to avoid foreclosure.
- Guarantee you will get the loan if you pay a fee upfront.
- Offer a suspiciously low or extremely high interest rate, or credit offers that don't mention the interest rate at all.



References

[1] European Central Bank (2024). Report on Payment Fraud. Frankfurt am Main: European Central Bank.

[2] European Union Agency for Cybersecurity (2024). ENISA Threat Landscape for Engineering and Financial Cyber Threats. Heraklion: ENISA.

[3] Europol (2024). Internet Organised Crime Threat Assessment (IOCTA). Luxembourg: Publications Office of the European Union.

[4] Federal Bureau of Investigation (2025). 2024 Internet Crime Report. Washington, D.C.: FBI Internet Crime Complaint Center.

[5] Federal Trade Commission (2025). Consumer Sentinel Network Data Book 2024. Washington, D.C.: Federal Trade Commission.

[6] Financial Action Task Force (2023). Cyber-enabled Financial Scams. Paris: FATF/OECD.

[7] INTERPOL (2024). Global Financial Fraud Threat Assessment. Lyon: INTERPOL General Secretariat.

[8] International Organization of Securities Commissions (2023). Retail Fraud and Regulated Entities. Madrid: IOSCO Technical Committee.

[9] Organisation for Economic Co-operation and Development (2023). Consumer Protection in E-Commerce and Digital Financial Fraud. Paris: OECD Publishing.

[10] World Bank (2022). Consumer Protection in Digital Financial Services: Enhancing Fraud Resilience. Washington, D.C.: World Bank Group.

[11] Regulamentul (UE) 2022/2554 privind reziliența operațională digitală a sectorului financiar (DORA).

[12] Strategia Națională de Educație Financiară – SNEF Romania 2024-2030.

[13] Educația tinerilor în scopul prevenției fraudelor financiare online, studiu realizat de Academia de Studii Economice din București (ASE) sprijinit de Raiffeisen Bank România