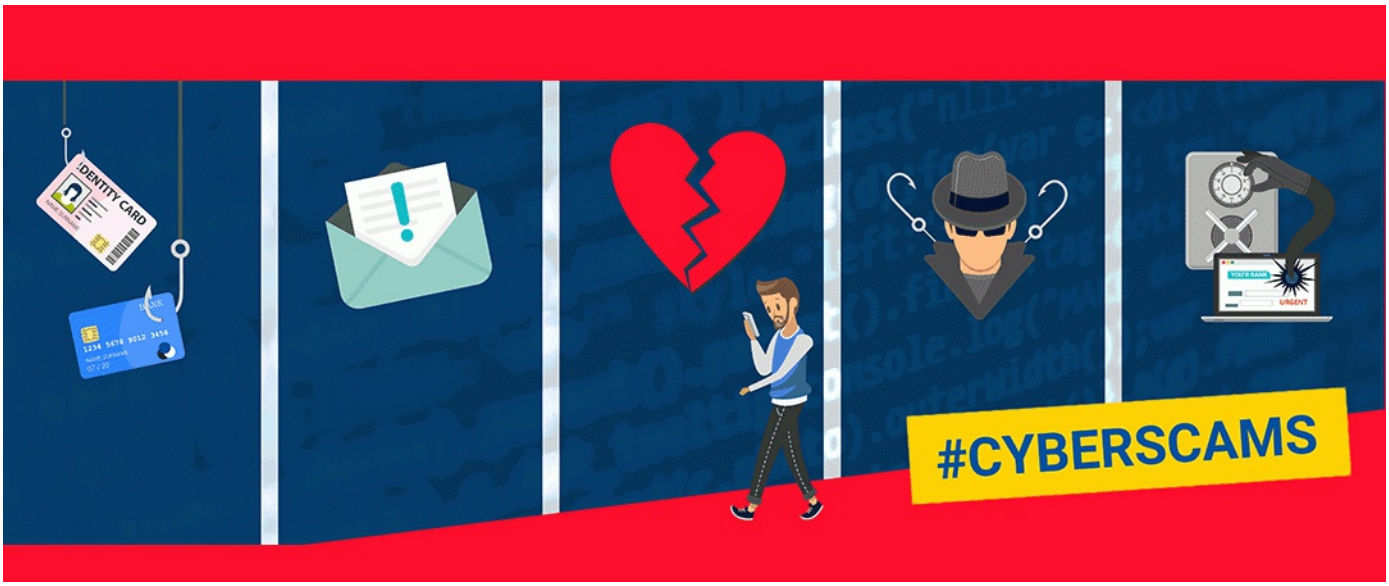
TAKE CONTROL OF YOUR DIGITAL LIFE. DON'T BE A VICTIM OF CYBER SCAMS!

Public awareness and prevention

7 most common online financial scams & how to avoid them



INFOGRAPHICS

- Spoofed Bank Websites
- Romance Scam
- Phishing / Vishing / Smishing
- CEO/Business Email Compromise (BEC) Fraud
- Investment Scams
- Invoice Fraud

Cybercriminals are constantly looking for ways to make money at your expense. Individuals and organisations often fall prey to frauds that involve various forms of social engineering techniques, where the information required is garnered from a person rather than breaking into a system.

These scams are typical examples of how cyber attackers can easily play on people's psychology and perceptions. The tips provided here are aimed to help you protect yourself. Awareness is your best defence!

General tips:

- Check your online accounts regularly.
- Check your bank account regularly and report any suspicious activity to your bank.
- Perform online payments only on secure websites (check the URL bar for the padlock and https) and using secure connections (choose a mobile network instead of public Wi-Fi).
- Your bank will never ask you for sensitive information such as your online account credentials over the phone or email.
- If an offer sounds too good to be true, it's almost always a scam.

- Keep your personal information safe and secure.
- Be very careful about how much personal information you share on social network sites. Fraudsters can use your information and pictures to create a fake identity or to target you with a scam.
- If you think that you have provided your account details to a scammer, contact your bank immediately.
- Always report any suspected fraud attempt to the police, even if you did not fall victim to the scam.

Download the Cyber Scams infographics in your language (PDF)

EU: Austria - DE | Belgium - FR NL | Bulgaria - BG | Cyprus - EL | Croatia - HR | Czech Republic - CS | Germany - DE | Denmark - DA | Estonia - ET | Finland - FI | France - FR | Greece - EL | Hungary - HU | Ireland - EN | Italy - IT | Latvia - LV | Lithuania - LT | Luxemburg - LU DE FR | Malta - MT EN | Netherlands - NL | Poland - PL | Portugal - PT | Romania - RO | Slovenia - SL | Slovakia - SK | Spain - ES | Sweden - SV | United Kingdom - EN Non-EU: Colombia - ES | Liechtenstein - DE | Norway - NO | Switzerland - DE FR IT | Ukraine - UK RU

SO HOW CAN THEY TRICK YOU?

1. THEY PRETEND TO BE YOUR CEO

CEO/Business Email Compromise (BEC) fraud occurs when an employee authorised to make payments is tricked into paying a fake invoice or making an unauthorised transfer out of the business account.

How does it work?

The method is based on an employee's eagerness to quickly carry out tasks when they are specifically requested to do so by senior management. The fraudsters appear to have considerable knowledge about the organisation and the emails appear very convincing.

What are the warning signs?

- Direct contact by a senior official through an unsolicited email or call.
- Request for absolute confidentiality.
- Pressure and sense of urgency.
- Unusual request in contradiction with internal procedures.
- Threats or unusual flattery and/or promises of reward.

WHAT CAN YOU DO?

AS A COMPANY:

- Be aware of the risks and ensure that employees are informed and aware too;
- Encourage your staff to approach payment requests with caution;
- Implement internal protocols concerning payments;
- Implement a procedure to verify the legitimacy of payment requests received by email;
- Establish reporting routines for managing fraud;
- Review information posted on your company website, restrict information and show caution with regard to social media;
- Upgrade and update technical security;
- Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

AS AN EMPLOYEE:

- Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure;
- Always carefully check email addresses when dealing with sensitive information/money transfers. Fraudsters often use copycat emails where only one character differs from the original;
- If you have doubts about a transfer order, consult a competent colleague, even if you were asked to use discretion;
- Never open suspicious links or attachments received by email. Be particularly careful when checking your personal mail boxes on the company's computers;
- Restrict information and show caution with regard to social media;
- Avoid sharing information on company hierarchy, security or procedures;
- If you receive a suspicious email or call, always inform your IT department.

2. THEY PRETEND TO BE ONE OF YOUR CLIENTS/SUPPLIERS

How does it work?

A business is approached by somebody pretending to represent a supplier/service provider/creditor. These approaches can be made over the telephone, by letter, fax or email. The fraudster requests that the bank details for a payment (i.e. bank account payee details) of future invoices be changed. The new account suggested is controlled by the fraudster.

WHAT CAN YOU DO?

AS A BUSINESS:

- Ensure that employees are informed and aware of this type of fraud and how to avoid it;
- Implement a procedure to verify the legitimacy of payment requests;
- Instruct staff responsible for paying invoices to always check them for any irregularities;
- Review information posted on your company website, in particular contracts and suppliers. Strongly advise your staff to limit what they share about the company and work place on their personal social media accounts;
- Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

AS AN EMPLOYEE:

- Verify all requests purporting to be from your creditors, especially if they ask you to change their bank details for future invoices;
- Do not use the contact details on the letter/fax/email requesting the change or verification. Use those from previous correspondence instead;
- Set up designated Single Points of Contact with companies to whom you make regular payments;
- For payments over a certain threshold, set up a dedicated system to confirm the correct bank account and recipient (e.g. a meeting with the company);
- When an invoice is paid, send an email to inform the recipient. Include the beneficiary bank name and the last four digits of the account to ensure security;
- Restrict information that you share about your employer on social media;
- Report the fraud attempts to your management or relevant department.

3.THEY CALL YOU, SEND YOU A TEXT MESSAGE OR AN EMAIL

Phishing (i.e. via email), smishing (i.e. via sms) and vishing (i.e. via voice call) are the most common social engineering attacks targeting bank customers.

Bank phishing emails

Phishing refers to fraudulent emails that trick the receivers into sharing their personal, financial or security information.

How does it work?

These emails:

- May look identical to the types of correspondence that real banks send, replicating the logos, layout and tone of real emails;
- Use language that transmits a sense of urgency, for instance implying a penalty if you don't respond;
- Can ask you to download an attachment or click on a link.

Cybercriminals rely on the fact that people are busy; at a glance, these spoof emails appear to be legitimate. As a result, recipients are more likely to take what is written in them seriously and act upon it.

WHAT CAN YOU DO?

- Keep your software updated, including your browser, antivirus and operating system.
- Be especially vigilant if the 'bank' email requests sensitive information from you (e.g. your online bank account password). A legitimate bank will only communicate with you securely through your online bank account.
- Look at the email closely: check for inconsistencies and anything that doesn't make sense:
- Look for slight differences in the sender's address: a zero could look like an "o".
- "Mouse over" the sender's address and look carefully at the actual sender: if possible, compare the sender's email address with previous real messages from your bank.
- Check for bad spelling and grammar mistakes.
- Don't reply to a suspicious email, instead forward it to your bank by typing in the address yourself.
- Don't click on the link or download the attachment, instead type -in the address in your browser.
- Watch out when using a mobile device. It might be harder to spot a phishing attempt from your phone or tablet. You can't "mouse over" a questionable link, while the smaller screen makes you less likely to spot obvious mistakes. If it's a bogus email, report it to your bank – all companies are eager to know about these scams. When in doubt, give your bank a call.

Bank vishing calls

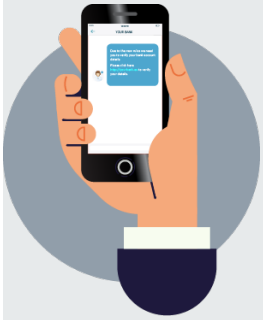
Vishing (a combination of the words voice and phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or into transferring money to them.

WHAT CAN YOU DO?

- Beware of unsolicited telephone calls.
- Take the caller's number and advise them that you will call them back.
- In order to validate their identity, look up the organisation's phone number (on their website or by running an online search) and contact them directly.
- Don't validate the caller using the phone number they have given you (this could be a fake or spoofed number).
- Fraudsters can find online basic information about you or your business (e.g. social media profiles). Don't assume a caller is genuine just because they

have such details.

- Don't share your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- Don't transfer money to another account on their request. Your bank will never ask you to do so.
- If you think it's a bogus call, report it to your bank.



Bank smishing SMSs

Smishing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message. They act as a trustworthy source, impersonating a bank, card issuer or utility/service provider.

How does it work?

The message will typically ask you (usually with a sense of urgency) to click on a link to a website or call a phone number in order to 'verify', 'update' or 'reactivate' your account. The website link will lead to a bogus website and the phone number to a fraudster pretending to be from the legitimate company. The goal is to get you to disclose any information that can then help the fraudsters steal your money.

WHAT CAN YOU DO?

- Don't click on links, attachments or images that you receive in unsolicited text messages without first verifying the sender. You can do so by searching the number online (if it is a scam, you might not be the first) or comparing it to the official number of the sender it claims to be originating from.
- Don't be rushed. Take your time and make the appropriate checks.
- Never respond to a text message that requests your PIN, online banking password or any other security credentials.
- If you think you might have responded to a smishing text and provided your bank details, contact your bank immediately.

4. THEY CREATE SPOOFED BANK WEBSITES

Bank phishing emails usually include links that will take you to a spoofed bank website, where you are requested to divulge your financial and personal information.

What are the signs?

Spoofed bank websites look nearly identical to their legitimate counterparts. Such websites will often feature a pop-up window asking you to enter your bank credentials. Real banks don't use such windows.

These websites usually display:

- Urgency: you will not find such messages on legitimate websites;
- Poor design: be cautious with websites that have flaws in their design or errors in spelling and grammar;
- Pop-up windows: they are commonly used to gather sensitive information from you. Don't click on them and do not submit personal data on such windows.

WHAT CAN YOU DO?

- Never click on links included in emails leading to your bank's website.
- Always type the link manually or use an existing link from your 'favourites' list.

- Use a browser that allows you to block pop-up windows.
- If something important really needs your attention, you will be alerted about it by your bank when you access your on-line account.
- If in doubt, give your bank a call

5. THEY PRETEND TO BE INTERESTED IN A ROMANTIC RELATIONSHIP

Romance scams commonly take place on online dating websites, but scammers often use social media or email to make contact.

What are the signs?

- Someone you have recently met online professes strong feelings for you, asking to chat privately.
- Their messages are often poorly written and vague.
- Their online profile is not consistent with what they tell you.
- They may also ask you to send intimate pictures or videos of yourself.
- They patiently wait to gain your trust, sometimes waiting up to weeks or months. Then they tell you an elaborate story and ask you for money, gifts or your bank account/credit card details.
- If you don't send money, they may try to blackmail you. If you do send money, they will ask for more.
- They will always have an excuse to justify their webcam is not working, being unable to travel to meet you and why they always need more money.

WHAT CAN YOU DO?

- Be very careful about how much personal information you share on social network and dating sites.
- Always consider the risks. Scammers are present on the most reputable sites.
- Go slow and ask questions.
- Research the person's photo and profile using online searches to see if the material has been used elsewhere.
- Be alert to spelling and grammar mistakes, inconsistencies in their stories and excuses such as their camera never working.
- Don't share personal pictures, videos or any compromising material that the scammers could later use to blackmail you.
- If you agree to meet in person, tell family and friends where you are going.
- Beware of money requests. Never send money or give credit card details, online account details, or copies of important personal documents.
- Avoid any arrangement with a stranger that asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or crypto currencies. It is rare to recover money sent this way.
- Don't transfer money for someone else: money laundering is a criminal offence.

If you are the victim of a

romance scam:

- Don't feel embarrassed, this scam happens more often than you can imagine;
- Stop all contact immediately;
- If possible, keep all communication (such as the chat messages) and any evidence that could help identify the fraudster;
- File a complaint with the police;
- Report it to the site where the scammer first approached you. Let them know the scammer's profile name and any other details that may help them to stop others being scammed;
- If you have provided your account details to a scammer, contact your bank or financial institution immediately.

6. THEY STEAL YOUR PERSONAL DETAILS VIA SOCIAL MEDIA CHANNELS

Your personal information is valuable to criminals. Protecting yourself from scams also means keeping your personal information safe and secure.

How does it work?

Even if you have your social media accounts configured as 'private' and properly protected, or if you are cautious and don't share much information within your profiles (pictures, videos, status updates, etc.), scammers use different techniques to trick you into typing in your personal details (name, email, password, credit card number, etc.), information which then can be used to steal your identity.

Your personal details can help fraudsters to:

- make unauthorised purchases on your credit card or open bank or telephone contracts and accounts;
- take out loans;
- sell your personal information to other fraudsters;
- carry out illegal business under your name.

Many attacks follow a similar pattern, some classic ones include:

- **Twishing** (a combination of the words Twitter and phishing) is the act of sending a message to a Twitter user directing them to visit a website. If the user logs in to the fraudulent site, the attacker obtains their account information (name and password).
- **Who viewed your profile or social media page?** Such service will request that you grant it access to your profile. It will then lead to a fraudulent survey, making you share your personal information. The spammer will earn a commission each time someone fills in the survey. You will never find out who looked you up.
- **"Is this you in this video?"** By clicking on these videos you will end up in a survey that earns money for the spammer. You could also end up infecting your device with malware.
- **"Your account has been cancelled", "confirm your email account".** Such scams aim to get you to disclose your private information and account credentials.
- **Gift card scams and fake offers from popular, high street names or high value brands.** These scams aim to get the user to reveal personal information or sign up for expensive services. They take up a new form every month and sound too good to be true - the requested service or product will never arrive.
- **Miracle product, free trials!** This online scheme uses free trial offers, bogus endorsements, and surveys to trick you into paying for products and subscriptions you don't know you are signing up for (e.g. recurrent shipping fees).
- **"Earn loads of money working from home".** Any job that requires a fee for you to start is likely to be fraudulent. These adverts are found on social media and they direct to an offer that charges for a kit that will help you get started on making thousands of euros. You can be asked for a lot of personal details, including your tax file number, copies of your passport or driving licence. Some job offers may be covers for illegal money laundering activities, asking that you receive payments into your bank account for a commission and then pass the money on to a foreign company. You will be acting as money mule for criminals, which is a crime.
- **Help, I'm in trouble!** An impersonator who pretends to be a relative in urgent need of money contacts you via social media message. The scammer will show distress and will ask you to wire him/her cash. Telephone, email or text message can be other ways of approaching you.

WHAT CAN YOU DO?

- Any time you want to verify information about a social media account, go directly to the site – do not trust a link that claims it will take you there.
- Be aware of how much information and pictures you share on social media sites. Fraudsters can use it to create a fake identity or target you with a scam.
- Review your privacy and security settings on each social media account. Take the time to understand exactly what your profile shows about you to the public.
- Do your online research. Search for the name of the product or the job offer to see what others are saying. You can combine it with words like "review", "complaint" or "scam".
- Report profiles you suspect to be scams to the social media platform. If they follow or befriend you, make sure you block them and cease to have any interaction.
- Regularly monitor your credit and debit card statements. If you are charged for something you haven't ordered, contact your bank and the card provider.

7. THEY MAKE YOU THINK YOU ARE ON TO A SMART INVESTMENT

Common investment scams may include lucrative investment opportunities such as shares, bonds, cryptocurrencies, rare metals, overseas land investments or alternative energy.

What are the signs?

- You receive an unsolicited call, repeatedly.
- You are promised quick returns and assured that the investment is safe.
- The offer is only available for limited time.
- The offer is only available to you and you are asked not to share it.

WHAT CAN YOU DO?

- Always get impartial financial advice before you hand over any money or make an investment.
- Reject cold calls related to investment opportunities.
- Be suspicious of offers promising a safe investment, guaranteed returns and large profits.
- Beware of future scams. If you have already invested in a scam, fraudsters are likely to target you again or sell your details to other criminals.
- Contact the police if you are suspicious.

… or present you with a great online offer!

Consumers and businesses are increasingly buying and selling online. Online deals are often a good buy, but beware of scams.

What can you do?

- Use domestic retail websites when possible – it will be more likely that you can sort out any problems.
- Do your research - check reviews before buying.
- Use credit cards – you have more chances of getting you money back.
- Pay only by using a secure payment service. Are they asking for a money transfer service or a wire transfer? Think twice!
- Pay only when connected to a secure internet connection – avoid using free or open public Wi-Fi.
- Pay only on a safe device. Keep your operating system and security software up to date.
- Beware of ads offering outrageous deals or miracle products. If it sounds too good to be true, it probably is!
- A pop-up ad stating you have won a prize? Think twice, you might just win malware.
- If the product doesn't arrive, contact the seller. If there is no answer, contact your bank.
- Always report any suspected fraud attempt to the police, even if you did not fall victim to the scam.

CRIME AREAS: Cybercrime

TARGET GROUPS: General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

ENTITIES: European Cybercrime Center (EC3)

Source URL: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/take-control-of-your-digital-life-don%E2%80%99t-be-victim-of-cyber-scams