ONLINE FINANCIAL FRAUDS AND SCAMS IN AN ARTIFICIAL INTELLIGENCE WORLD

STAY ALERT AND PROTECT YOURSELF

Online financial frauds and scams are not new, but Artificial Intelligence (AI) has made them smarter and harder to spot. Criminals now use fake messages and websites, false celebrity profiles, and even AI-generated voices or videos that look like your banker, your friends or your family to trick you.

They often reach out to you via social media, emails, unexpected calls, and messaging apps that sound real.

You may face risks such as financial loss, identity theft, and emotional distress. Be cautious and follow these key tips to stay safe:

Stay alert to existing online financial fraud and scams powered by AI,
e.g., impersonation, phishing, investment and insurance scams, and even romance fraud and scams. To learn more about different types of fraud and scams see page 5 to 7.

For more about fraud and scams specific to crypto see the dedicated factsheet on crypto fraud and scams ( ).

Spot warning signs:
Learn to recognise suspicious behaviours, messages or offers (see page 2);

Protect yourself:
Secure your personal information (see page 3); and

Know what to do if you fall victim to fraud or scams
(see page 4).

Warning signs

A Promise that seems too good to be true.

An unexpected call from an unknown number.

An urgent request for money or personal information, including from someone pretending to be a family member, a friend, or even a public figure.

A request to take control of your device, download an app, scan a QR code or click on a link.

A request for personal information or banking details (e.g. passwords, credit card numbers, internet banking credentials, or security codes).

A request for payment via untraceable methods (e.g. cryptos, gift cards, wire transfers, or prepaid debit cards).

A suspicious or incorrect email address or link (e.g. spelling errors in the URL or unusual web addresses).

An attachment from an unknown source, especially .exe, .scr, .zip, or macro-enabled Office file (.docm, .xlsm).

Poor grammar or formatting in an official-looking document, although AI may allow fraudsters to mask these flaws more effectively.

A website that looks professional but lacks verified contact details or company registration information.

Intonation that sounds unnatural, lacks pauses and seems overly fluent or robotic. Pay attention to ‘voice cloning’, although AI generated speech may also sound very natural.

Videos where the voice may sound robotic or overly smooth, lip movements and facial expressions may be misaligned with the speech, or background, lighting and shadows may be inconsistent. These are often AI-generated videos (deepfakes).

Steps to protect yourself

1 **Never share personal or banking information:**

Legitimate companies will never ask for your PINs, passwords, internet banking credentials, or security codes by email, text, social media, or phone.

2 **Pause and think before you act:**

Don't rush into sending money, sharing information, or clicking on links- scammers deliberately create a sense of urgency (e.g. IT issues with your bank, emergency calls involving your friends and family members, threatening language etc.). In case of any doubts, even minor, do not act; end the call and verify the source or identity carefully.

3 **Check the source/identity carefully:**

- Always verify where messages, calls, emails, and links come from- even if they look official, seem to come from a friend or your family, or even a public figure. For example, call or text your family and friends using a known number via a trusted channel; look for spelling errors, strange URLs, or missing security indicators (e.g. verify that the website link includes an 's' in 'HTTPS' to make sure the website is secure, and check for any added or missing letters in the company name).
- Don't open links from unsolicited messages, install only official applications through trusted app stores, and don't scan unknown QR codes.
- Agree with your family on a 'safe word'- a secret phrase you can use to confirm identity if someone with a familiar voice calls you with an urgent request for money and claims to be a family member (e.g. parents, sister/brother, child).
- Use verified contact details to reach the company or individual directly and never rely on the contact information provided by the suspected fraudster (e.g. search for the company name independently, use verified business directories, previously confirmed contact methods). Scammers might claim to be authorised or mimic the website of an authorised company. Verify whether any warnings have been issued by your national financial authority or included in the IOSCO I-SCAN list (iosco.org/i-scan/). For crypto providers, check if they are authorised in the EU (e.g., check the ESMA register ( ).

4 **Pay attention to potential AI tricks:**

As AI technology advances, scams are becoming more convincing than ever- even with the best security tips. If something feels unusual or you detect any of the warning signs outlined above, stop and reassess.

5 **Never install remote access software or share your screen:**

Banks and financial institutions will never request that from you.

6 **Keep devices and accounts secure:**

Use strong and unique passwords, keep them secret, and avoid reusing the same credentials on different platforms. Enable multi-factor authentication where possible. See some passwords tips here ( ). Keep your software and antivirus protection up to date and activated.

7 **Be cautious with unexpected and limited-time investment opportunities:**

If it sounds too good to be true, it probably is.

8 **Think before you share information on social media:**

Chat groups, forums, social media posts and photos can be valuable sources of knowledge for fraudsters. Revealing too much about yourself or your investments can make you an easy target.

What to do when you have become a victim of fraud or scam

Immediately stop transactions

To block any further transfers to suspicious accounts and avoid additional losses. Stop all contact with the scammers – ignore their calls and emails and block the sender.

Contact your bank or financial company:

Inform your bank or financial company immediately via official contact channels, to explore options for freezing or reversing transactions.

Change your passwords on all your devices and apps/websites.

Fraudsters buy leaked passwords online and try them on multiple accounts. Changing just one password is not enough; make sure to change all of them, so fraudsters cannot re-use them.

Report and alert:

Report the incident to the police or your national financial authority (http://www.mfsa.mt) and inform your network (e.g. friends and family) to raise awareness. These actions can help you protect yourself and others.

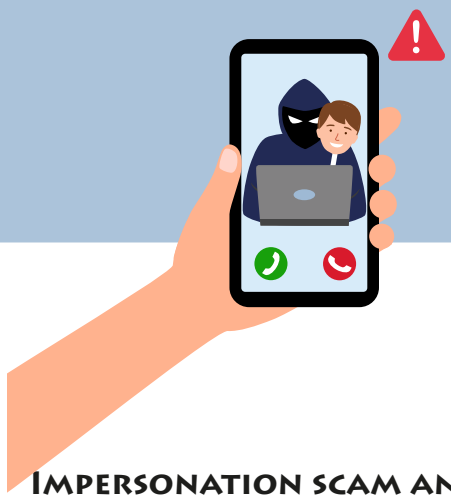
Beware of 'recovery room' fraud:

The fraudster may contact you knowing that you are a victim of a previous scam, claiming to be a public authority (e.g., police, tax or financial authority etc.) and offering to recover your lost money for a fee. This is often another attempt to scam you. Remember: being scammed once does not prevent you from being scammed again.

European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities and Markets Authority, 2025
Luxembourg: Publications Office of the European Union, 2025

PDF ISBN 978-92-9407-282-5 doi:10.2853/2531487 DZ-01-25-170-EN-N

TYPES OF ONLINE FINANCIAL FRAUDS AND SCAMS POWERED BY AI



Impersonation scam and use of deep fake

You receive an unexpected call from someone claiming to be your bank, a public authority (e.g. police, tax or financial authority etc.), an insurance distributor, an IT company, or even a family member. The caller might urge you to transfer funds to keep them safe, citing suspicious activity on your account or your insurance policy. They might also ask you to disclose your banking details (e.g. payment card number, internet banking credentials, or passwords), click on a link, or install a software, pretending it can quickly solve the issue. The caller might use a falsified number, often matching your bank's phone number to appear legitimate (spoofing).

Scammers may use AI to create fake videos, images, or audio that mimics someone's voice (e.g. your banker or a family member), face (e.g. a celebrity), or movements. **This is known as 'Deepfake'.**

What might happen:

By mentioning personal details and creating a sense of urgency, the scammer tricks you into actions you didn't intend to take - such as sending money to their account, clicking on a malicious link, or installing a malware on your device. This can give the scammer direct access to your banking credentials. With this information, they can change your password, access your bank account, and steal your money. Remember: just because a caller knows personal details about you doesn't mean he/she is trustworthy.

Phishing and social engineering

You receive an email or message that seems to come from your bank or a financial company, warning you of 'suspicious activity' on your account. The logo, layout, and language look professional, and the message might appear in the same thread as other conversations from your bank. The message urges you to click on a link to verify your account or reset your password. The link leads to a fake website that looks identical to your internet banking. Without realising it, you enter your details into a website designed to steal your personal information.

Scammers use AI to craft convincing phishing messages by analysing social media data to identify their victims and adapting the content for each target.

What might happen:

The scammer accesses your bank account and steals your money or creates a fake profile with your personal details to commit fraud.

Investment or insurance scam

You see an advertisement on social media or a website promoting a 'limited-time investment opportunity with low risks' or 'limited-time discount' on an insurance from a well-known company. The ad features a celebrity's photo and recommendations that are often fake. After expressing interest by clicking on a link or filling in a form, you are contacted and redirected to a platform or messaging channel where you receive professional-looking advice and documents. You are encouraged to invest a small amount, followed by larger sums, or to pay the premium into what seems to be a secure account.

Fraudsters use AI tools to make these fake proposals or emails highly convincing and difficult to detect. They also use AI-powered social media bots to create fake accounts that interact with you, spread misinformation, and simulate real behaviours to gain trust and influence your decisions.

What might happen:

After trying to withdraw your money or make a claim, the contact stops responding. You discover that the company does not exist or that the insurance risk is not covered. You then realise that you have sent money directly to a scammer as part of a fraudulent scheme. Unfortunately, you cannot get your money back, and your personal and financial details can be used to commit further fraud (e.g. signing contracts on your behalf which might lead you to lose even more money).

Romance fraud and scam

You have been contacted on social media, dating apps, or by phone/text by someone you have not met in real life. This person engages in frequent, personal and romantic conversations, building trust using fake profiles. Over time, the conversation shifts toward money or financial opportunities, such as crypto-investments with promises of high returns and low risk. The person asks you to transfer money to an account or guides you through setting up an account and making a small initial deposit to make the scheme look legitimate before encouraging you to invest more.

Fraudsters use AI to generate fake profiles, identify their victims on social media/dating apps using data you made available, or use chatbots to generate messages.

What might happen:

The scammer extracts as much money as possible, then cuts off all communication and disappears. The fraudulent investment website or app is taken offline, leaving you unable to access the supposed investments. In addition to financial loss, the personal information you shared might be used to target your friends and family or for identity theft which can have financial or legal consequences for you (e.g. the fraudster could make purchases, take loans in your name, or you might be held responsible for debts or crimes committed under your name until proven otherwise).

Purchase scam

You come across an attractive deal for a purchase on an online marketplace. The company offering the deal requests a payment outside the official platform, claiming it uses a 'secure payment system', and sends you a link to complete the purchase. The link redirects you to a fraudulent bank authentication page that imitates the official website of the bank and uses its logo and design, so you enter your online banking details to make the payment.

Scammers use AI to create highly convincing fake bank websites, order confirmations, and invoices. AI helps them mimic the tone, branding, and style of real companies. In some cases, they use AI chatbots to answer questions and make the deal seem more believable.

What might happen:

The payment through a third-party link bypasses the marketplace's protections. The scammer obtains your login information to your bank account and steals your money.