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, messaging apps, emails and unexpected calls 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, 6 and 7.

More on fraud and scams specific to crypto see Crypto fraud and scams factsheet (https://link.europa.eu/mdhmybjd).

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

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

Know what to do if you fall victim to fraud or scam
(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 (shorturl.at/zZwVI).

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 (shorturl.at/7ns3I). 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 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.

Luxembourg: Publications Office of the European Union, 2025
PDF ISBN 978-92-9407-207-8 doi:10.2853/7159167 DZ-01-25-093-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 risk you insured 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.

European Banking Authority

European Insurance and Occupational Pensions Authority

European Securities and Markets Authority

CRYPTO FRAUDS & SCAMS

STAY ALERT AND PROTECT YOURSELF

The fast growth of crypto-assets and their specific features – global accessibility, speed, anonymity, and often irreversibility of transactions – make you a prime target for cybercriminals. Fraudsters and scammers use sophisticated tactics to trick you, such as 'Ponzi schemes', fake investment opportunities, free offers on social media and false messages. They also use romance investments scams or look-alike addresses to poison your wallet. They often reach you via social media, messaging apps, emails and unexpected phone calls which 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 possible crypto fraud and scams:
To learn more about different types of frauds and scams
(see page 5, 6, 7 and 8)

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

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

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

Warning signs

A promise that seems too good to be true.

An unsolicited offer.

A guaranteed fast and high return.

Urgency for action (e.g. limited-time offers that pressure you to act immediately).

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

An invitation to click on a link, scan a QR code or download an app.

A request to send or share private keys and seed phrases (list of words to access and recover your crypto wallet).

Suspicious or incorrect URL.

Logo with slight distortions, a website that copies the look of a real company's website or looks professional but lacks verified contact details, company registration information, track record, or verifiable presence.

Unknown exchange platform.

A suspicious attachment, especially .exe, .scr, .zip, or macro-enabled Office file (.docm, .xlsm).

Steps to protect yourself

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

Don't rush into investing, sharing information, or clicking on links – scammers deliberately create a sense of urgency. In case of any doubts, even minor, do not act or invest and verify the source carefully.

2 **Check the source carefully:**

- Always verify where the 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. 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.
- Even if an offer looks official, always cross-check it against the company's website or check the social media account is verified (e.g. with official checkmarks).
- 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). Scammers might claim to be authorised or mimic the website of an authorised company. You can verify if the crypto provider is authorised in the EU by checking the ESMA register (shorturl.at/zZwVI). You can also consult your national financial authority's website to see if any warnings or blacklists have been issued or the IOSCO I-SCAN list (iosco.org/i-scan/).

3 **Never share passwords, private keys, or seed phrases:**

Anyone with access to them can take control of your assets. Legitimate companies will never ask for your passwords or security codes by email, text, or phone.

4 **Keep devices and private keys secure:**

Use strong and unique passwords for each of your crypto accounts, keep your password secret, and avoid reusing the same credentials on different platforms. Enable multi-factor authentication where possible. See some passwords tips here (shorturl.at/7ns3I) [replace with national links if applicable]. Keep your software and antivirus protection up to date and activated.

5 **Be cautious with unexpected investment offers:**

Be wary of investments promising huge returns. If it sounds too good to be true, it probably is.

6 **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.

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.

Disconnect and revoke access:

Revoke suspicious permissions in your digital agreement that run automatically on the blockchain (smart contract) to stop scammers from spending your tokens without your consent. Many wallets and blockchain explorers offer tools that allow you to see which smart contracts currently have access to spend your tokens. To do so you can:

- use a trusted 'permission checker', which verifies whether a user or blockchain address is authorised to execute an operation.
- review the list of approvals, and
- use the 'revoke' button directly from the platform.

Move your funds:

If your wallet is compromised, immediately transfer your remaining assets to a new secure wallet.

Contact your crypto provider:

Inform your crypto provider as soon as possible using official contact channels, to explore potential options. Even if, in most cases, reversing the blockchain transaction will not be possible, the provider might still freeze the scammer's account (if it is on their platform) and blacklist the wallet address.

Report and alert:

Report the incident to the police or your national financial supervisory authority, and inform your network (e.g. friends and family) to raise awareness. These actions are the best way to protect yourself and others.

Beware of 'recovery room'-fraud:

The fraudster may contact you as 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.

See the Joint European Supervisory Authorities warning to learn more about the risks related to crypto-assets (https://link.europa.eu/hcFpGj) and the factsheet 'Crypto-assets explained: What MiCA means for you as a consumer' (https://link.europa.eu/BRv4Gn).

Luxembourg: Publications Office of the European Union, 2025
PDF ISBN 978-92-9407-206-1 doi:10.2853/7409327 DZ-01-25-092-EN-N

Types of crypto-scams

'Pump and dump' scheme or 'rug pull'

You see an advertisement (ad) on social media or a website promoting a 'limited-time investment opportunity' in crypto, recommending investing in a new crypto token or project. After expressing interest, you are contacted and redirected to a crypto-exchange platform or messaging channel (e.g. Telegram, Viber, or WhatsApp). A seemingly credible contact promises quick profits or high returns if you invest promptly. You are encouraged to invest a small amount and then pressured to invest more.

What might happen:

You discover the invested token is worthless and the contact you have been in touch with stops responding. When you try to withdraw your money, the website no longer exists, and the company is unreachable. Scammers artificially inflated or overstated a low-value crypto to increase its value ('pump'), then sold off their assets ('dump'), causing the value to crash and leaving investors with losses. Alternatively, they might shut down the project and disappear with the funds ('rug pull').

Impersonation scam

After you posted a question on a social media platform or a website about a crypto wallet issue, you receive an unexpected direct message (DM) or an email from someone pretending to be a trusted contact (e.g., a crypto-exchange, wallet provider, IT support, or even a friend). The person asks for your seed phrase (i.e. sequence of words that serves as the central backup for accessing your digital wallet), passwords, or private keys (an automatically generated cryptographic code that proves ownership of digital assets).

What might happen:

Once you share your seed phrase, passwords, or private keys, the scammer uses them to steal your crypto or other funds. Keep in mind that losing private keys results in the permanent and irreversible loss of access and ownership to your crypto-assets. Unlike bank transactions, in case of crypto transfers, once your funds are gone, recovery is nearly impossible.

Phishing

You receive an unexpected message via email, phone, pop-up, or social media, claiming to be from a well-known crypto-asset provider. The message invites you to log in or download a new app. You might also receive an email that appears to be from your crypto wallet app, urging you to resolve a security issue by clicking on a link provided by an unofficial source, or by updating the app.

What might happen:

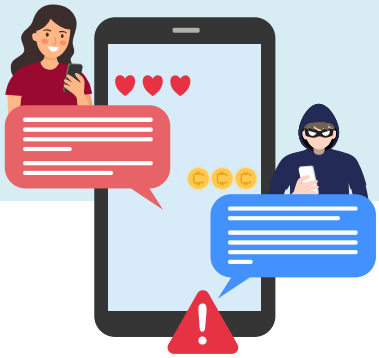
By clicking on the link, downloading the app, or scanning a QR code, you install a malware that allows the scammer to access and use the information to steal your crypto-assets or your funds.

Giveaway scam

You come across an announcement on social media claiming companies are giving away crypto-assets after a small crypto investment. They include a video or a post featuring photos of a celebrity or a brand – usually fake or obtained without authorisation – promising to "double your crypto" if you send money first. The logo, layout, testimonials, and language used look professional and official, as does the website you are redirected to.

What might happen:

After sending your crypto, you receive nothing in return, and you have lost the sent money. The giveaway was fake, and the post or livestream impersonating celebrities or companies was designed to deceive you.



Romance investment scam

You have been contacted on social media, dating apps, or phone/text by someone you have not met in real life. This person may engage in frequent, personal and romantic conversations, building trust using fake profiles. Gradually, they steer the conversation toward financial opportunities, claiming huge profits from crypto-investments and encouraging you to invest with promises of high returns and low risk. They guide you through setting up an account and making a small initial deposit to make the scheme seem legitimate.

Scammers create fake online profiles and use stolen or Artificial Intelligence-generated pictures to approach you.

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 with no access to the supposed investments. In some cases, scammers may use the information obtained during the scam to target your friends and family and commit identity theft which can have financial or legal consequences for you (e.g. the fraudster can verify stolen wallets in your name and you might be held responsible for debts or crimes committed under your name until proven otherwise).

Ponzi scheme

You are invited to take part in a project that promises consistent high returns from crypto-asset investments, often backed by testimonials or fake success stories. The scheme may be presented as a multi-level marketing opportunity, where you earn rewards not only from your own investment, but also by recruiting others. Early investors appear to receive payouts, encouraging more people to join and promote the scheme.

In reality, there is no genuine business or profit being generated. Instead, the money comes solely from the contribution of newer investors which is utilised to pay returns to the scheme's organisers and first participants.

What might happen:

Once new investments slow down, the scheme collapses, and you, like most participants, lose your money. The organisers disappear, leaving no way to recover funds. The multilevel structure helps the scam spread quickly, as victims unknowingly become promoters.

A LOOK-ALIKE ADDRESS WHICH IS POISONING YOUR WALLET

After making a crypto transaction, you notice a new address appearing in your wallet history. This address looks similar to one you have previously interacted with. Scammers can make fake wallet addresses appear in your transaction history by sending a tiny amount of crypto from a look-alike address to your wallet. You end-up storing in your wallet's recent activity or auto-suggestions the fake address created by the scammer. Scammers deliberately create look-alike addresses by changing only a few characters, often in the middle of the address, to avoid detection.

***What might happen**:*

When you try to send crypto and copy the wrong address from your wallet history, you unknowingly send funds to the scammer's wallet. Because crypto transactions are often irreversible, your funds are lost in most of the cases permanently. This scam relies on visual deception and user error, exploiting the habit of copying and pasting wallet addresses without close inspection.