Deepfake and AI Scams

What they are, how they are used, and how to protect yourself

Created in partnership by Deep Truth Project & Friends Against Scams (National Trading Standards)

What is a deepfake?

A deepfake is a fake video, voice or photo of a real person, made using artificial intelligence (AI). It can show someone saying or doing things they never did. AI can also invent people who don't exist at all.

These fakes are cheap and easy to make. A criminal can copy someone's voice from a few seconds of a video posted online. Criminals also use AI to write scam messages in perfect English, by the thousand.

These fakes are very convincing. Research shows even careful listeners cannot reliably tell a cloned voice from a real one. Being blindsided by one says nothing about your intelligence. This factsheet shows you how criminals use them, and the simple habits that beat them.

How deepfakes are being used in scams

Family phone scams

The phone rings. It's your daughter's voice. She's upset, she's in trouble, and she needs money now. She asks you not to tell anyone.

The voice is exactly hers, because it was copied. AI can clone a voice from a few seconds of audio taken from videos online. Criminals use cloned voices to fake family emergencies. In the cruellest version, the voice cries or screams and someone demands money for their safe return.

Remember: a familiar voice is no longer proof of who is calling.

WHAT TO DO: Hang up. Call the person or organisation back on a number you already have. It takes a minute and it is effective against this scam. For extra security, use a different phone for the call back, if possible, as sometimes the criminals can keep the line open after you think you have ended the call. Better still, agree a family code word in advance that a criminals could not know.

Fake calls from your bank, the police or HMRC

A caller says they are from your bank's fraud team, the police or HMRC. The voice sounds professional. The number on your screen even matches the real organisation, because caller ID can be faked. They say your account is at risk, and you must move your money to a 'safe account', or read out a code, right now.

Remember: safe accounts do not exist. No real bank or police officer will ever ask you to move money, and a caller knowing your details or 'passing security' proves nothing.

WHAT TO DO: Hang up. Wait a few minutes, then call back on a number you found yourself: dial 159 to be connected securely to your bank, 101 for the police, or use the number on an official letter. The request to move money is itself the scam.

Identity theft: when the fake is you

Criminals don't only fake celebrities and loved ones. With a few photos and a voice clip taken from social media, they can pretend to be you: passing voice-recognition phone banking, or fooling the photo checks used to open accounts, so that loans and bank accounts are set up in your name. The National Trading Standards Scams Team has also seen friendly 'survey' calls used to harvest personal details and record people's voices, and cloned voices used to fake a victim's agreement to payments.

Warning signs: letters about accounts you never opened, entries on your credit report you don't recognise, or debt collectors contacting you out of the blue.

WHAT TO DO: Be careful with 'surveys' that ask for personal details and think before posting voice notes and videos publicly. Check your credit report for free with the credit reference agencies, especially after any data breach. If your details have been stolen, Cifas Protective Registration puts a warning flag on your name. You can also ask your bank to switch off voice ID.

Celebrity investment scams

You see a video online. A famous money-saving expert is recommending an investment. He looks real and sounds real. But he never said it. Criminals made the video using AI. Fake celebrity adverts are one of the most common deepfake scams. They mostly promote investment schemes, and sometimes health products or prize draws.

Remember: genuine investments are not promoted through celebrity videos. If a famous face is selling you an investment online, it is fake.

WHAT TO DO: Never click the advert. Check any investment on the FCA register at www.register.fca.org.uk and check for warnings on the FCA's Warning List of Unauthorised Firms at www.fca.org.uk/consumers/warning-list-unauthorised-firms. Check any product on the shop's own official website.

Fake celebrity health products

The same fake-video machinery is used to sell products: miracle cures, diet gummies, pain devices. Trusted TV doctors have been faked at scale to promote health products they have never heard of. The product never arrives, is worthless, or hides a repeating card payment.

Remember: real medicines are never sold through celebrity social media adverts. Never stop or swap a prescribed medicine for something advertised online. The harm here can be to your health, not just your wallet.

WHAT TO DO: Check the person's own official website; many post warnings about fake adverts using their name. If you have already bought, contact your card provider about getting the payment back and cancel any repeating payment.

Romance fraud

You meet someone online. You message for months. You even see them on video calls. Then comes a crisis, a visa problem or a medical bill, and they need your money. Criminals now use AI to make fake profile photos that look completely real. They can even fake a live video call, putting a false face over their own. So, seeing someone on video no longer proves they are real.

Watch for the pattern instead:

1. The relationship moves very fast.
2. They can never quite meet you in person.
3. Sooner or later, they ask for money.

WHAT TO DO: Never send money to someone you have not met in person, no matter how real they seem. Talk to someone you trust before acting. The request for money is the scam.

Fake intimate images (sextortion)

A message arrives. It contains an intimate photo of you, except you never took it. The sender threatens to share it with your family, friends or workplace unless you pay.

Criminals can now use AI to fabricate intimate images from ordinary photos taken from social media. The image is fake, but the fear is real, and that fear is the whole scam. Paying does not make it stop. It marks you as someone who will pay.

Remember: the image doesn't need to be real to be a crime, and it is never the victim's fault.

WHAT TO DO: Do not pay and do not reply. Keep the evidence: messages, usernames, images. Report it to the platform and to the police. Adults can get free, confidential help from the Revenge Porn Helpline (https://revengepornhelpline.org.uk) and can use https://stopncii.org/ to help stop images spreading. If the person targeted is under 18, contact the police or Child Exploitation and Online Protection service at https://www.ceop.police.uk

Scam emails and texts

An email arrives from your bank. Perfect English. Your name. The right logo. An urgent problem, and a link to fix it. AI wrote it, along with thousands of others that same morning. Scam messages used to give themselves away with spelling mistakes. Not anymore.

Remember: a well-written message proves nothing. Look at what the message asks you to do. Urgency, links and requests for details are the real warning signs.

WHAT TO DO: Never use the link or phone number in the message. Go to the organisation directly, using the number on your card or by typing their official website yourself. Forward scam texts to **7726** (free) and scam emails to **report@phishing.gov.uk**.

Fake "proof"

Criminals also use fake photos and videos as proof in all kinds of scams: a video tour of a rental flat that doesn't exist, photos of a puppy that was never for sale, a live video of a celebrity giving away money. A video is no longer evidence. The rule is always the same: judge the request, not how real it looks.

You may have heard you can spot deepfakes by looking for glitches or odd movements. Don't rely on this. The technology improves every few months, and good fakes blindside even experts and online tools that claim to detect AI make mistakes too.

The real red flags are not in the picture or the voice. They are in the behaviour:

1. Urgency: you must act right now.
2. Secrecy: don't tell anyone, don't check with anyone.
3. A request: for money, personal details, codes or images.
4. Pressure: they don't want you to check. That is itself the biggest warning.

However real it looks or sounds, judge the request.

Protect yourself: five things to set up today

1. Agree a code word with your family that a criminal could not know.
2. Save the real numbers of your bank and close family, and remember 159: the safe way to reach your bank's fraud team from any phone.
3. Make a rule: no urgent money request gets an answer within the hour. Real emergencies survive a pause. Scams don't.
4. Check things some other way, using a number or website you already know is real.
5. Tell the people around you about these scams. Someone who has heard of voice cloning is very hard to scam with it.

Supporting victims

Victims of these scams often feel a special kind of shame. "But I heard his voice." "But I saw her on video." If someone tells you this happened to them, believe them. Remind them that these scams are designed to deceive anyone. Being targeted is never their fault.

Then help them act fast:

1. Contact the bank first: call 159 or the number on their card. If they were manipulated into transferring money, banks must consider refunding them under rules introduced in October 2024, in many cases up to £85,000.
2. Report it to Report Fraud on 0300 123 2040 or at reportfraud.police.uk. In Scotland, report to Police Scotland on 101.
3. Tell Citizens Advice on 0808 223 1133. Reports feed intelligence straight to Trading Standards, who can act against the scam.
4. Keep the evidence: messages, numbers, adverts, and the original files rather than screenshots where possible.
5. Warn them about the 'second wave': after a scam, criminals often call back pretending to be police or a company that can recover the stolen money. That call is the same criminals. Real organisations never cold-call offering to recover funds for a fee.
6. If their own voice or photos have been misused, report it to the platform where it appeared, and use the specialist help listed in the sextortion section above.

When supporting someone who has been a victim of AI based scams, make sure to approach without blame — victims are often embarrassed or ashamed. Listen first; avoid saying "I told you so" or questioning their judgment. Help them take the practical steps listed above.

Key takeaways

There is a scam out there for everyone. Seeing and hearing are no longer proof. Checking is. Every scam ends with a request. Judge the request. Hang up, call back, go direct. Talking about these scams protects people. Tell someone today.

Want to do more?

Friends Against Scams runs the SCAMchampion programme, which trains individuals to help protect others in their communities. Consider joining the programme to help safeguard people in your community.

Friends Against Scams — www.friendsagainstscams.org.uk — Scam awareness and prevention for individuals, communities and professionals.

Citizens Advice — citizensadvice.org.uk — General advice including scams and fraud, available to anyone in the UK, free and confidential.

Age UK — ageuk.org.uk — Scam awareness, prevention and victim support for people aged 50+ and those who support them.