OFFICE OF THE POLICE & CRIME COMMISSIONER FOR SURREY

Question EVERYTHING

The dangers of AI and deepfakes

How to avoid becoming the victim of AI generated scams

What is an AI generated scam?

An AI generated scam uses artificial intelligence (AI) to misrepresent someone or something to deceive a victim for personal gain of money or property. Fraudsters rely on computer technology to create realistic fake images, videos, voices or convincing messages to manipulate their victims causing loss or risk of loss to them.

This so-called synthetic media looks real and can be very difficult to distinguish from genuine media.

Fraud is the most prevalent crime against individuals in England & Wales estimated at 41% of all crimes reported

(Source: Crime Survey of England and Wales September 2024)

What is a deepfake?

Police and Crime Commissioner Lisa Townsend
Deepfake vs genuine – can you tell the difference?

Deepfakes are pictures, video or audio clips that have been generated or manipulated by artificial intelligence to look real. They can be used by scammers to spread disinformation, deceive and cause harm.

Deepfakes can show a real person doing or saying something that they have not done so in real life. This can include high profile public figures and celebrities as well as everyday people. Fictional characters can also be created. Deepfakes can target you personally or a mass audience.

In 2024, more than £10 million was lost by victims after being convinced by deepfakes that featured influential people advertising fake investment schemes

(Source: Action Fraud)

Question EVERYTHING

Watch the Question EVERYTHING film and see a deepfake of Police and Crime Commissioner Lisa Townsend, here:
surrey-pcc.gov.uk/question-everything-fraud/

“Don’t believe everything you see and hear”

AI and investment fraud: Deepfakes can be used in false advertising to promote fake investments, often by impersonating public figures.

AI and romance fraud: AI is used by scammers to create fake profiles on dating websites or social media platforms. Posing as genuine people looking for companionship, the aim is to build trust and then ask to ‘borrow’ money.

AI and extortion: Deepfakes can be created by fraudsters that publicly humiliate their victims by manipulating their image to convey them in a vulnerable state or performing an explicit act. The intention by the perpetrators is to blackmail and extort money, known as ‘sextortion’.

AI and voice spoofing scams: Scammers generate voicemails or social media audio clips pretending to be a friend or relative requiring money in an emergency. Victims can act on impulse hearing a familiar voice in need.

AI and fraudulent websites, emails and texts: Scammers can use AI to create realistic looking communications from banks, pension providers and other official bodies. These fraudulent websites and messages can ask you for personal information including bank details or invite victims to make payments.

There is a deepfake attempt every five minutes

(Source: Entrust Annual Identity Fraud Report 2025)

How to protect yourself: Think AI scam

Stay safe online Scammers can use AI to trawl social media to manipulate pictures, videos and personal details for deepfake content so be careful what you share publicly. Protect your accounts with strong, unique passwords that use three random words. Turn on 2-step verification (2SV) for important accounts which provides an extra layer of security that only you can access. Search for 'Stop Think Fraud 2SV' for more information via **gov.uk/StopThinkFraud**

Unexpected contact Scammers use AI to power phone calls, emails, texts and WhatsApp messages that look genuine. If someone contacts you out of the blue claiming to be from a trusted service, hang up or reject the messaging platform that you have been contacted on, and contact them back via a method that you know for sure is genuine.

Scrutinise websites Scammers build AI generated copycat websites of trusted companies that look almost identical to the real thing. Check the web address and contact details for anomalies and the content for any misspellings or irregularities.

Unsolicited emails Scammers generate emails using AI so beware of unfamiliar senders, messages urging you to act quickly or suspicious links and attachments. Always verify the sender's address or phone number by calling the company using the number on their official website.

Online dating Scammers use AI to write messages, send videos and voice notes to build a rapport with you. Be mindful if there is an avoidance to meet in person, the relationship moves forward quickly, or if money is requested because of an emergency. Fraudsters might also encourage you to move the conversation away from the original platform to avoid being detected.

More than half of the population age 16+ (53%) are not confident in their ability to identify a deepfake

(Source: You Gov poll for Ofcom, June 2024)

Deepfake videos: Be vigilant

Verify authenticity of any famous person advertisement
Be wary of investments schemes that are promoted by any famous person as these deepfakes are designed to look real. Research independently and check if the financial services firm is authorised by the Financial Conduct Authority (FCA) for the services being offered and that the contact details match those listed on the FCA Firm Checker: **fca.org.uk/consumers/fca-firm-checker**

Top 3 famous people currently impersonated by fraudsters:

Martin Lewis
Elon Musk
Richard Branson

(Source: Action Fraud, November 2025)

Double check legitimacy of any video Scammers can create hyper-realistic video of 'family members' or 'friends' in distress to manipulate people into sending money. Pause, think and verify the communication independently through a trusted separate channel to confirm the validity of the request.

Voice spoofing: Listen carefully

Test if the voice is from a real person If you are being contacted from a 'loved one' asking for money in an emergency, call them back directly on their known number to confirm that it really is them.

Alternatively, you could ask the voice on the end of the phone for exacting details of a shared memory to see if they know the answer or set up a family code word to verify whether the person is really who they say they are.

You must never prompt a caller by giving any personal information away. Scammers can mask the number they're calling from and can even appear to be calling from your friend or family member's number, so beware.

Criminals can clone a person's voice from as little as 3 seconds of audio and manipulate it to say whatever they want

More than 1 in 4 (28%) of UK adults think they have been the target of an AI voice cloning scam in the last year

(Source: Mortar research for Starling Bank, August 2024)

AI criminals operate like traditional fraudsters...

With urgency
The fraudster will insist that you act quickly to prevent you from consulting others or verifying the request.

Insist on secrecy
The fraudster might tell you to not share the communication with anyone, claiming confidentiality or concern for others.

Manipulative behaviour
Communication is carefully designed to evoke fear, panic, or enthusiasm to overshadow better judgement and bypass usual security checks.

Unusual payment methods
Scammers typically request payment by untraceable routes, such as wire transfers, cryptocurrency, or gift cards because these methods are hard to reverse.

If you are a victim of fraud, please keep in mind...

Identity theft
If you suspect that your identity has been stolen, check your credit report promptly using a trusted online service. It's good practice to review your credit rating every few months and investigate any unusual or unexpected activity.

Repeat victim scams
Fraudsters sometimes contact previous victims, claiming they can help recover lost money. This is a secondary scam. Never engage with these callers: hang up immediately and do not share any personal information.

Highest loss by an individual this financial year so far to AI-enabled fraud has been in the region of £500,000

(Source: National Fraud Intelligence Service, November 2025)

"Fraud is this country's most common crime, with scammers targeting individuals ruthlessly and mercilessly.

"Scam techniques have become increasingly slick and sophisticated with the proliferation of AI. Now that fraudsters can generate such realistic deceptive content in minutes, it's important to arm yourself with the information that you need to protect you and your families".

Lisa Townsend, Police and Crime Commissioner of Surrey

You are not alone

If you think that you have been a victim of fraud, report it to **Action Fraud**:

Call 101 or 0300 123 2040 | Textphone 18001 101 |
Online **actionfraud.police.uk**

Received a suspicious email? Forward it to **report@phishing.gov.uk**

Received a suspicious text? Forward it free of charge to 7726

Received a suspicious call? Send a text free of charge to 7726 with the word 'Call' followed by the scam caller's number.

There is support

Surrey Police: Call 101

Victim and Witness Care Unit: **victimandwitnesscare.org.uk** or phone: 01483 639949

(Open 9am – 5pm. Calls charged at standard rate)

Stop! Think Fraud: **gov.uk/StopThinkFraud**

Question EVERYTHING

Produced by

OFFICE OF THE POLICE & CRIME COMMISSIONER FOR SURREY

Supporting partners

Surrey Community Safety and Prevention Board

Victim & Witness Care Unit
Supporting those affected by crime in Surrey

Information current as of November 2025