NATIONAL TRADING STANDARDS

Protecting Consumers
Safeguarding Businesses

AI SCAM WATCHLIST

The top ten AI-enabled scams posing a threat to consumers, and how they work



INTRODUCTION

Artificial intelligence (AI) is transforming the way criminals target consumers. From cloned voices and deepfake videos to highly personalised phishing messages and fake online shops, AI is enabling criminals to create scams that are more convincing than ever, and on a massive scale.

Rather than creating new types of scams, AI is accelerating the industrialisation of fraud, enabling organised criminals to deceive and defraud more people, more quickly and with less effort.

This Watchlist highlights the key AI capabilities criminals now have in their 'toolkit' to amplify the impact of their crimes.

We then set out the most significant AI-enabled scams being seen by those working in the consumer protection landscape, based on a range of evidence including: National Trading Standards (NTS) intelligence logs and cases; evidence from the Chartered Trading Standards Institute (CTSI) and input from various partner organisations.

We explain briefly what these scams are, how AI is super-charging them and then outline the key steps consumers can take to protect themselves.

THE AI CRIMINAL TOOLKIT

Behind almost every scam in this Watchlist are the same handful of AI capabilities. Understanding these helps explain why fraud is becoming harder to spot.

DIGITAL HUMANS

WHAT IT IS

A lifelike, AI-created virtual person that is broadcast online and can sometimes interact with humans in real time, simulating natural conversation and human expressions.

USED ACROSS...

Potential for use across almost any scam as they can hold convincing conversations and build relationships over time.

DEEPFAKE VIDEO

WHAT IT IS

AI can analyse existing images and videos of a person to create realistic fake footage that can imitate their appearance, gestures and speech.

USED ACROSS...

Family impersonation scams, investment scams (footage of celebrities), sextortion (fake intimate videos).

VOICE CLONING

WHAT IT IS

With just a short recording, AI can copy someone's voice closely enough to allow criminals to make fake phone calls or voice messages.

USED ACROSS...

Family impersonation scams, Banking scams – such as setting up unauthorised direct debits.

AI-GENERATED WEBSITES

WHAT IT IS

AI can clone trusted websites or create brand new sites that look polished and professional in rapid time and at low cost.

USED ACROSS...

Many types of scam including shopping, holiday, property, recruitment, investment, tech support and charity scams.

FAKE REVIEWS

WHAT IT IS

Convincing reviews written at scale by AI to make products, services or businesses appear more trustworthy or popular than they really are.

USED ACROSS...

Shopping scams, rogue trader scams.

AI CHATBOTS

WHAT IT IS

AI-powered conversational tools that can communicate naturally with people, allowing criminals to answer questions and build trust.

USED ACROSS...

Many types of scam including shopping, investments, tech support, recruitment, holiday and ticketing scams.

AI-GENERATED MESSAGES

WHAT IT IS

Using AI to produce error-free, personalised phishing emails, text messages and social media scams on a huge scale.

USED ACROSS...

Recruitment, romance, property, investment and charity scams.

AI-GENERATED IMAGES

WHAT IT IS

AI can create realistic photos of products, properties, vehicles or documents that make fake adverts and listings appear genuine.

USED ACROSS...

Many types of scam including shopping, holiday, property, romance, investment, ticketing and charity scams.

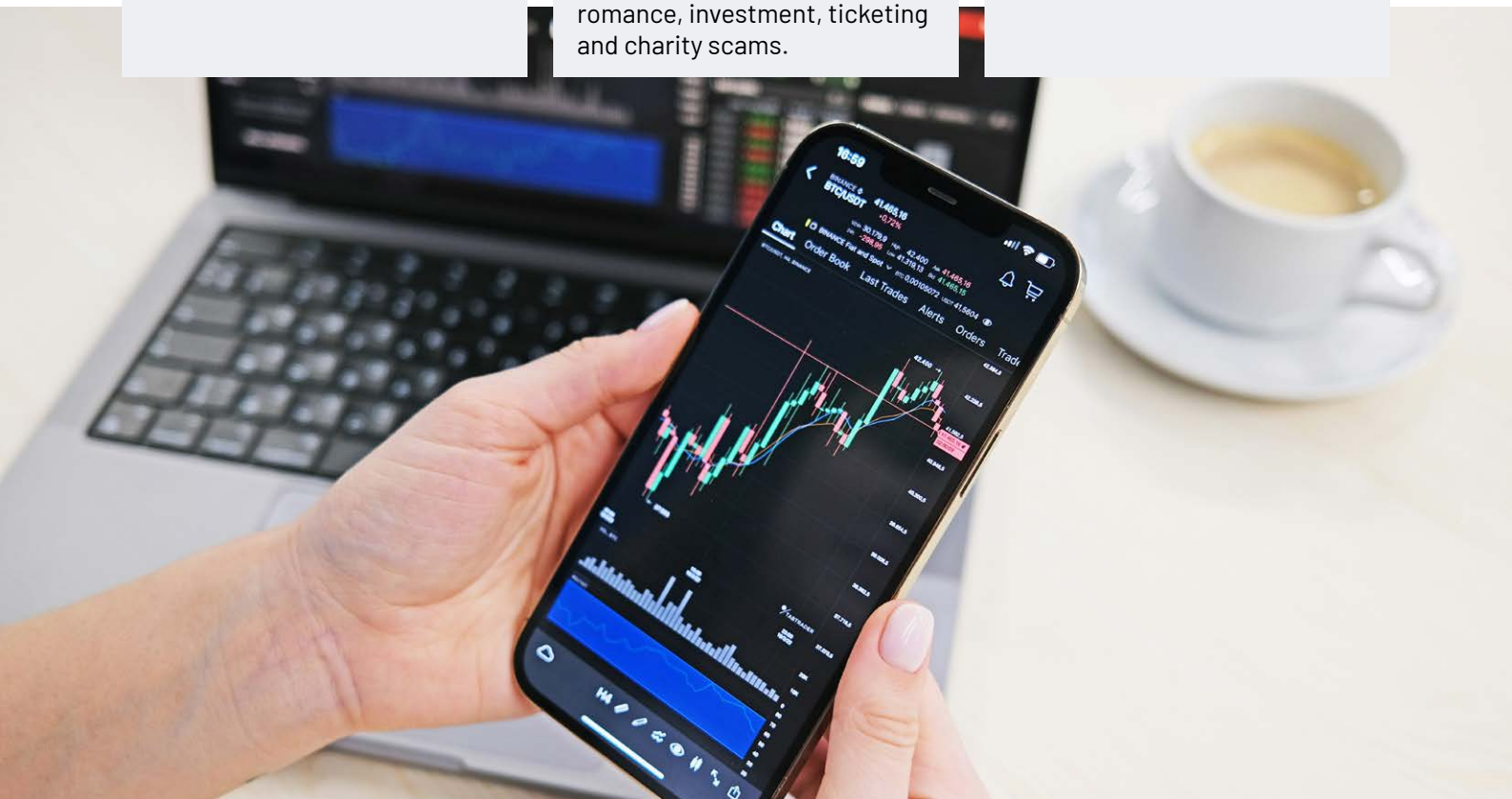
POISONED AI SEARCH

WHAT IT IS

When criminals 'poison' the information used by AI systems, causing AI search results to direct users to fake websites.

USED ACROSS...

Any scam involving a fake website.



01 AI SHOPPING SCAMS



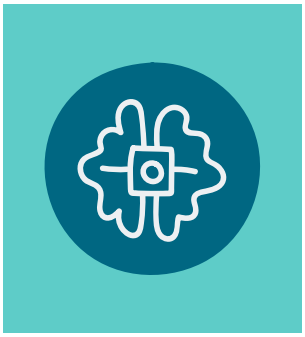
WHAT YOU'LL SEE

Convincing copycat websites that look like trusted major brands, or online shops for retailers that don't actually exist. These often claim to be family-owned firms selling quality UK-made goods, with images often featuring the 'owners' and UK high streets with Union Jack flags.



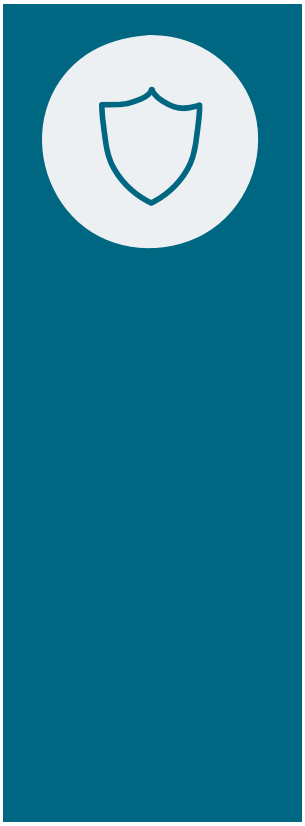
HOW YOUR MONEY IS STOLEN

You order a product that either never arrives, or is a cheap, mass-produced item from countries such as China. Criminals steal your payment and may also use your card details for further fraud, sell them on to other criminals, add you to a data harvesting list to target you with further scams.



WHY AI MAKES IT CONVINCING

Criminals can use AI to create convincing online shops, copycat brand websites, customer reviews and customer service chatbots at speed. They may copy a genuine retailer, or invent a business that looks established and trustworthy, then use limited time offers to pressure people into buying. It's even possible that digital humans could be used to 'front' these fake companies.



PROTECT YOURSELF

- Check the URL (website address). Use several website safety checkers (such as Get Safe Online, Scam Adviser or Ask Silver) if you're unsure
- Use reverse image search to check whether photos are copied from genuine retailers
- Look for reviews from a range of independent sources, not just those on the site itself
- Be wary if prices seem too good to be true
- Check for an address and contact details and verify these on an online map. Also check the delivery and returns policy – often the so-called 'local' firm is based abroad e.g. in China
- Be cautious if you're pressured to buy quickly through countdown timers, 'limited stock' claims or flash sales
- Pay by credit card where possible, or use a trusted payment service. Avoid paying by bank transfer

02 AI JOB SCAMS



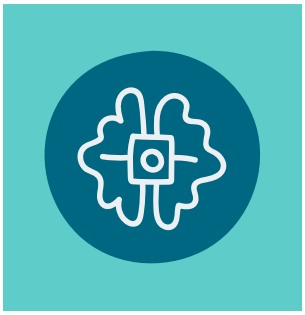
WHAT YOU'LL SEE

Job adverts that look legitimate, but use scraped ads from genuine sites – or entirely AI-generated ads. The application and interview process look professional but are completely faked.



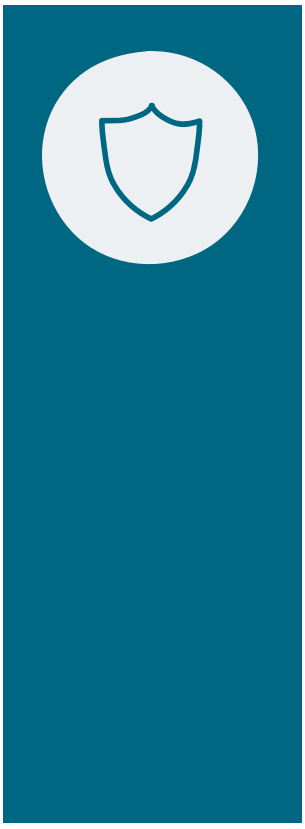
HOW YOUR MONEY IS STOLEN

During the recruitment process you are asked to pay money e.g. for equipment or admin costs – but the job is not real. You may also be added to a data harvesting list to target you with further scams.



WHY AI MAKES IT CONVINCING

Criminals can create real-looking job adverts, recruiter profiles, application forms and personalised messages with AI. They may copy a genuine employer or recruitment agency website, or invent a company that looks credible, then use automated emails, chatbots or video interviews to take victims through a fake recruitment process.



PROTECT YOURSELF

- Even if the ad is on a well-known recruitment website, check the employer's official website and LinkedIn page
- If you're unsure, contact the employer directly to check the vacancy is genuine
- If the job is not for home working, check and verify the address
- Never pay upfront fees for DBS checks, training, equipment, visas or admin costs as a condition of being offered the job
- Be wary if you're offered a job unusually quickly or without a proper application or interview process

03 AI INVESTMENT SCAMS



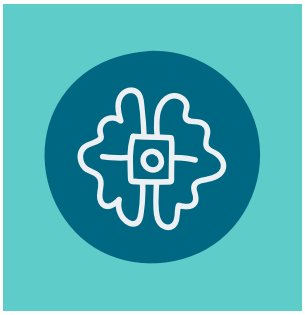
WHAT YOU'LL SEE

Convincing celebrity endorsements, adverts and videos promoting fake cryptocurrency, trading or investment schemes, hosted on slick-looking websites.



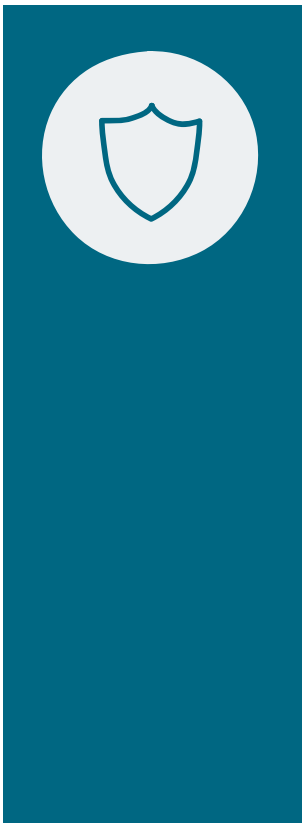
HOW YOUR MONEY IS STOLEN

You are persuaded to 'invest' money, usually a small amount to start with. You might even see a 'return' paid out – but this is a ruse to build trust and encourage larger payments.



WHY AI MAKES IT CONVINCING

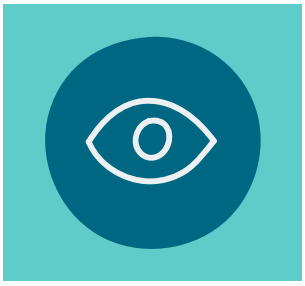
AI can be used to create realistic investment websites, trading platforms, adviser profiles, adverts and personalised messages. They may copy genuine financial firms or use deepfake videos of celebrities apparently endorsing a scheme. They then use chatbots, fake dashboards and claims of time-limited returns to pressure victims.



PROTECT YOURSELF

- Be wary of cold-calls, messages and adverts promoting investments with high or guaranteed returns, including cryptocurrency, property, fine wines and other commodities.
- Research independently – check the company, the investment and the adviser. The Financial Conduct Authority (FCA) runs the Firm Checker, where consumers can check if a company is authorised to provide financial services, as well as providing a warning list which flags firms or individuals operating without permission
- Be cautious of celebrity endorsements as they could be faked
- Don't be pressured into a decision – take time to think and consider talking to an independent financial adviser that you've found yourself
- If you have already invested and have doubts, don't send more money – even if the online dashboard appears to 'prove' your investment is growing. Stop, seek advice and report it

04 AI ROMANCE OR ‘BEFRIENDING’ SCAMS



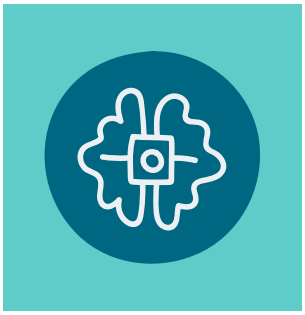
WHAT YOU’LL SEE

Attractive profiles on social media or dating apps, which are used to engage victims and begin ‘relationships’ or ‘friendships’ using fake messages, photos and video calls.



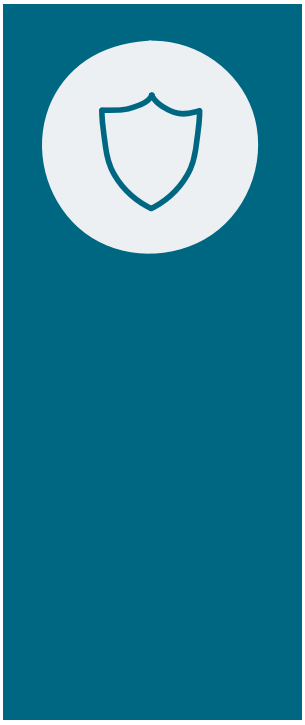
HOW YOUR MONEY IS STOLEN

Once trust is built, criminals posing as your romantic partner or good friend will create an emotional or emergency story to pressure you into ‘lending’ them money.



WHY AI MAKES IT CONVINCING

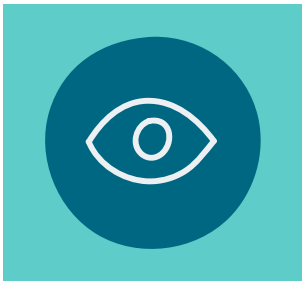
AI can be used to create fake dating profiles, photos, messages, voice notes and video-style calls. They may invent a believable identity, use AI to remember personal details and keep conversations going over weeks or months.



PROTECT YOURSELF

- Use reverse image search to check whether their profile photos are stolen from elsewhere
- Be wary if someone expresses strong feelings very quickly, especially if they are avoiding meeting you in person.
- Don’t assume someone is genuine because you’ve spoken to them by phone or video – these can easily be faked
- Never send money, gift cards or personal or financial information to someone you have not met in person

05 AI TRAVEL AND TICKET SCAMS



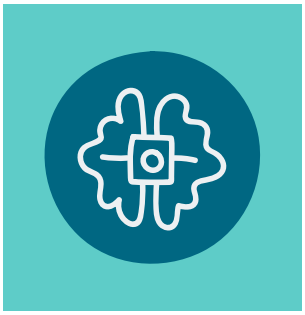
WHAT YOU'LL SEE

Glossy airline, holiday accommodation and event booking websites, advertised on social media or via emails and text, displaying deals that seem too good to be true.



HOW YOUR MONEY IS STOLEN

You pay a significant sum, perhaps not realising the holiday or event ticket isn't real until you turn up at the airport or venue – and the travel agent or ticket seller is long gone.



WHY AI MAKES IT CONVINCING

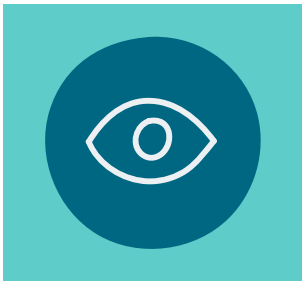
Criminals can use AI to create enticing fake travel or ticketing websites in minutes, backed up by social media ads, fake reviews and human-like chatbots.



PROTECT YOURSELF

- Check the URL (website address) to ensure the agency is genuine. If you're unsure, use reputable website checkers such as Get Safe Online, Scam Adviser or Ask Silver
- Compare prices across well-known providers and be wary of deals that seem too good to be true
- Check reviews from independent websites, not just the company's own website
- Don't be pressured into booking immediately even if it looks like a special offer is 'about to end' or tickets are 'almost sold out' – these are scam red flags
- Pay by credit card if you can – avoid paying by bank transfer
- Check that travel companies have the right financial protection, such as ATOL for package holidays or ABTA membership where applicable

06 AI TECH SUPPORT SCAMS



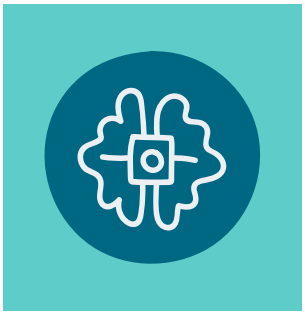
WHAT YOU'LL SEE

Urgent calls, emails, text messages or pop-up security warnings designed to convince people that their computer or bank account has been hacked or infected with a virus.



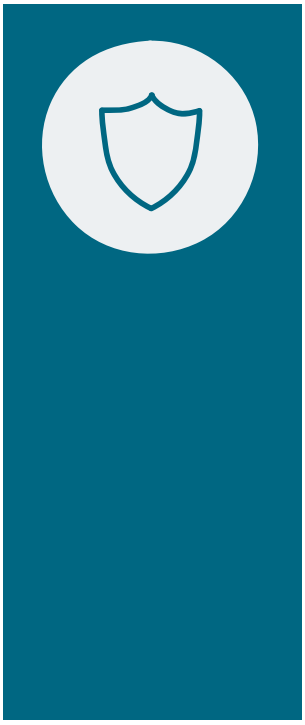
HOW YOUR MONEY IS STOLEN

The fear that your device or bank account has been compromised means you are quickly convinced to pay money, share passwords or provide remote access to your computer. This allows personal information and further money to be stolen.



WHY AI MAKES IT CONVINCING

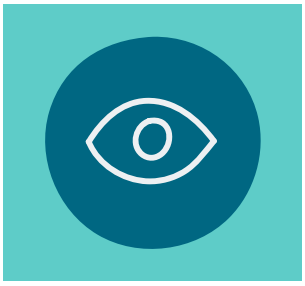
Convincing support websites, pop-up security warnings and chatbots that appear to offer technical help, can all be made using AI.



PROTECT YOURSELF

- Genuine software companies and technology providers won't contact you out of the blue asking for passwords, one-time security codes or remote access to your device
- If you get an unexpected security warning, stop and verify it. Contact the company directly via its official website or app – never use the phone number or link in the message or pop-up
- Never give anyone remote access to your computer or phone unless you're certain they are genuine

07 AI IMPERSONATION SCAMS



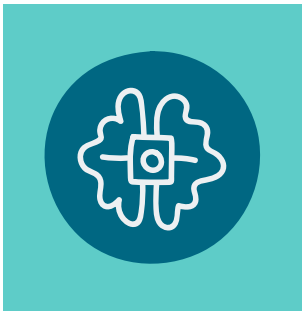
WHAT YOU'LL SEE

Someone the victim trusts, such as their child or a good friend, contacts them asking for money to help them in an emergency, either via a text message, voice message, phone call or video call.



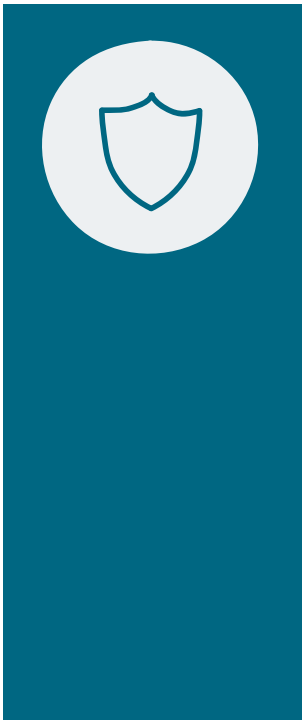
HOW YOUR MONEY IS STOLEN

By creating an urgent and emotionally charged scenario, you are pressured into believing your loved one needs immediate financial help.



WHY AI MAKES IT CONVINCING

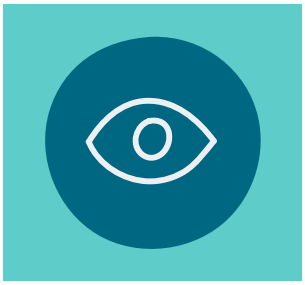
Criminals use AI-generated deepfake videos and voice-cloned audio to impersonate family members or close friends.



PROTECT YOURSELF

- Don't assume someone is genuine just because you've heard their voice or seen them on a video call
- Stop and verify their identity before sending money. Call them back using a trusted number or contact them another way
- Consider agreeing a family 'safe word' or 'passphrase'. Choose something random that only your family knows, and use it to verify genuine emergency requests for money or help

08 AI ROGUE TRADER SCAMS



WHAT YOU'LL SEE

An online or social media advert, or a profile on an 'approved trader' platform that looks professional and is highly rated with maximum stars and plenty of good reviews.



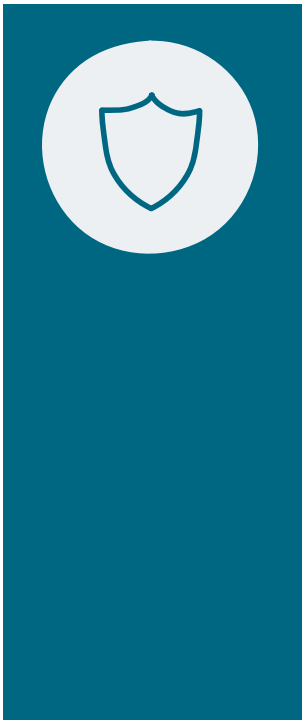
HOW YOUR MONEY IS STOLEN

You may be asked to pay a small deposit to secure the job. The criminal will then come to your home and charge inflated prices either to carry out very little work or work of a poor quality. If you complain or request your money back, you may be ignored or threatened.



WHY AI MAKES IT CONVINCING

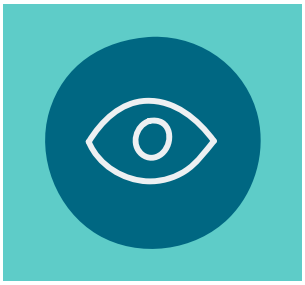
Criminal 'rogue traders' can use AI to create business profiles, social media accounts and fake reviews, allowing them to pose as established firms with many satisfied customers. Criminals often create several business profiles under different names, allowing them to target multiple consumers at the same time.



PROTECT YOURSELF

- Don't rely on professional-looking websites, reviews or social media recommendations when choosing a tradesperson
- Check your council website for any local 'approved trader' lists
- Use TrustMark, the UK Government-endorsed quality scheme for tradespeople working in and around the home
- Ask your family, friends or neighbours for recommendations
- Always get at least three quotes so you can compare prices and pick up on anything that doesn't look right

09 AI CHARITY SCAMS



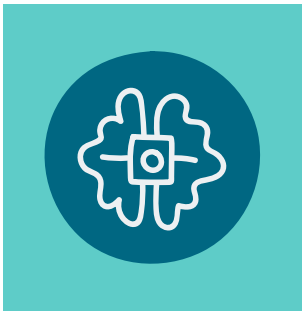
WHAT YOU'LL SEE

Professional-looking charity websites, email appeals that falsely use the name of real charities or fake appeals on crowdfunding sites.



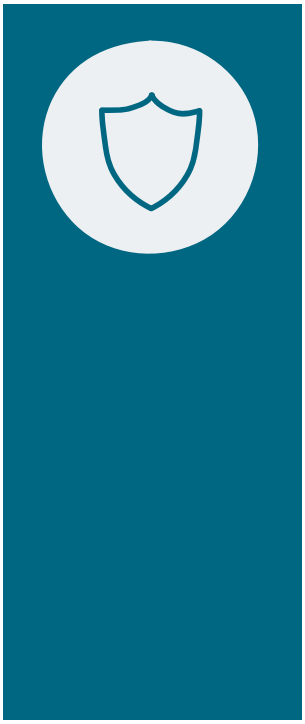
HOW YOUR MONEY IS STOLEN

You respond to an emotional appeal for a good cause by donating money – and you may be added to a data harvesting list to target you with further scams.



WHY AI MAKES IT CONVINCING

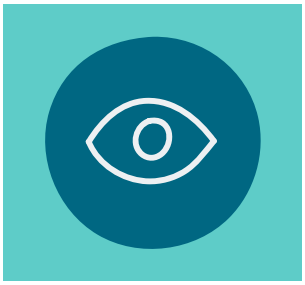
Criminals can use AI to create highly emotional appeals at speed, including fake charity websites, realistic donation pages, personalised emails, social media posts and images that appear to show people affected by a disaster or tragedy. They may copy a genuine charity, or invent a charity that looks credible.



PROTECT YOURSELF

- Beware of unexpected requests for donations, particularly after major disasters or tragedies when criminals often exploit people's generosity
- Verify the charity before donating. Check the charity register, held by the Charity Commission, and follow its advice on how to donate safely
- Make sure you're using the charity's official website. If you clicked on the link in an email, message or social media post, go back and search for the charity yourself or type its web address into your browser
- If you're unsure, use reputable website checkers such as Get Safe Online, Scam Adviser or Ask Silver

10 AI RECOVERY SCAMS



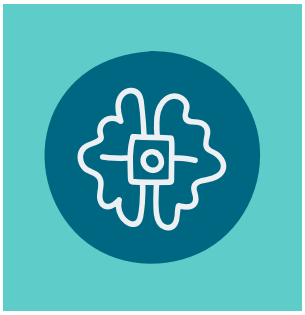
WHAT YOU'LL SEE

A person who has already lost money to fraud is contacted again by someone claiming they can help recover their stolen money. Criminals may pose as police officers, government agencies, regulators, investigators, lawyers or specialist recovery firms.



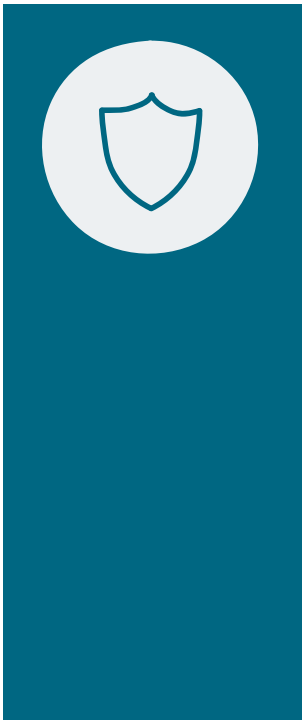
HOW YOUR MONEY IS STOLEN

The criminals will persuade you that in order to recover your stolen money, they will need a fee upfront, or will need your bank details to pay the money into. They will take your money and keep asking for more, and if they have your bank details they'll empty your account.



WHY AI MAKES IT CONVINCING

Criminals can use AI to create professional-looking recovery websites, legal emails, investigator profiles, chatbots and voice or video impersonations of officials.



PROTECT YOURSELF

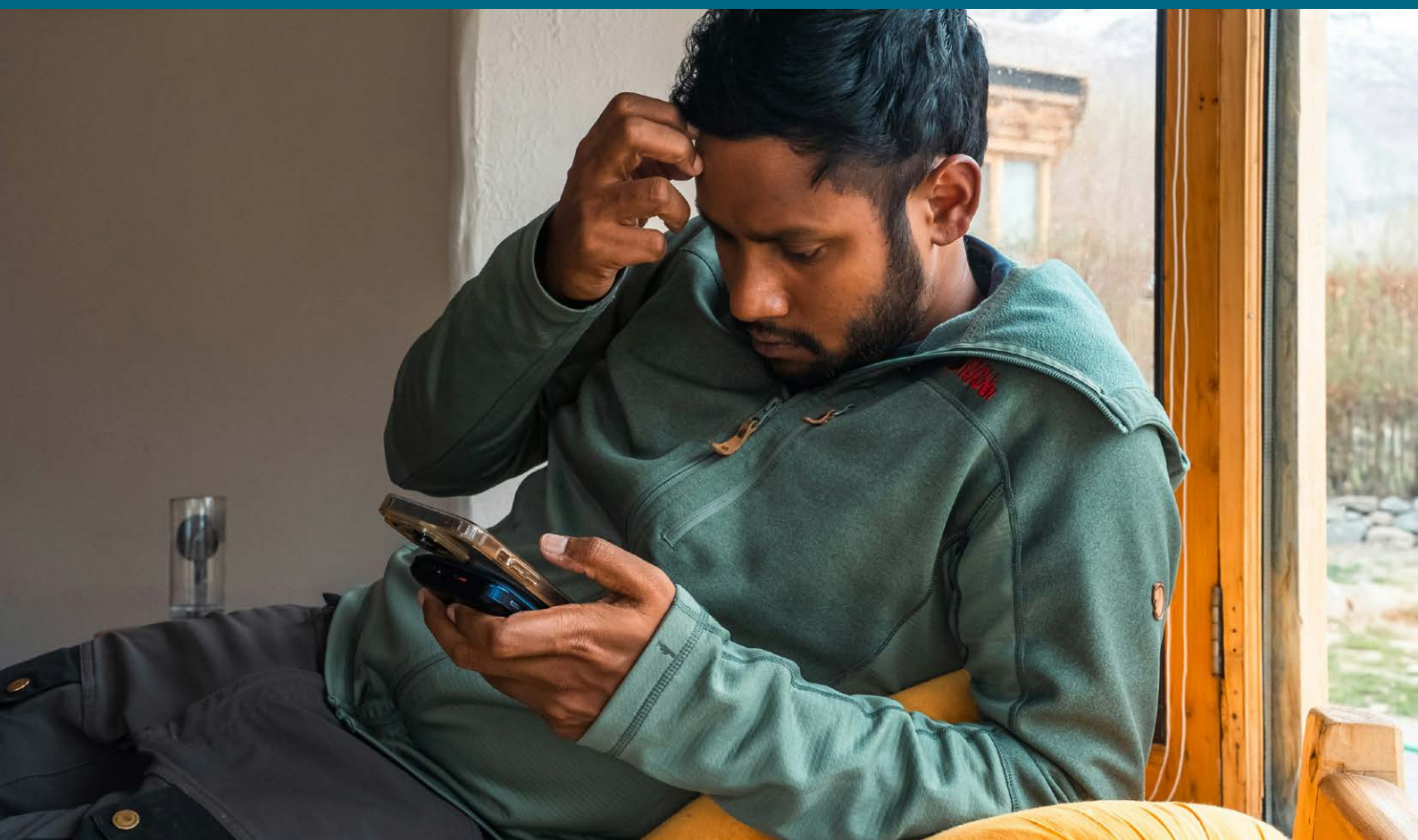
- If you've recently been a victim of a scam, be aware that you may be targeted by offers of help to recover your money – even if the person seems to know details of the original scam
- Don't pay any more money and never share bank details, passwords or security codes. Genuine authorities or companies will not ask you to pay a fee to recover stolen money

CONCLUSION

Although AI is a positive development in many ways and has huge potential to be used for good, some of those same features that make it helpful for use in professional and home settings are exactly why the threat from criminal use is so great, especially with parallel AI systems without ethical safeguards already known to be operating on the dark web.

Key themes that run throughout all AI scams in this Watchlist:

- **AI technology makes it easier than ever to commit fraud.** Criminals no longer need significant technical expertise to create highly sophisticated scams.
- **Fraud is becoming increasingly automated.** Organised criminals can target thousands of victims simultaneously, creating scams on a massive scale.
- **Complex scams can be built in minutes.** What would have taken days and significant expertise can be created with just a few prompts – then removed, tweaked and rebuilt just as quickly.
- **Scams are becoming more convincing than ever.** The professional-looking nature of AI-assisted scams means consumers can't rely on the traditional warning signs such as poor spelling or awkward language to spot them.
- **Consumers can no longer rely on seeing or hearing something as proof that it is genuine,** as AI-generated images, voices and videos become increasingly realistic.
- **Criminals can hide more effectively.** As AI creates the whole fabric of the scam, from words to pictures, video and voice, the criminals themselves are many steps removed, making enforcement more challenging than ever.



LOOKING AHEAD

Advances in AI technology are paving the way for a new generation of organised criminals who will need little technical expertise to equip themselves with increasingly advanced tools. We can expect to see scams becoming ever more sophisticated, deployed at speed and on a massive scale. Looking ahead, AI-enabled crime is also expected to become increasingly autonomous, with specially programmed AI agents capable of carrying out complex fraudulent activity with minimal human involvement, making scams even harder to identify and stop.

There is no doubt that AI presents considerable opportunities for the enforcement sector, enabling efficiencies and working alongside human expertise in supporting investigations, enforcement and legal proceedings. When used for good, it will be a very powerful tool and will help to address the threat posed by criminals across the board.

But as fast as we can counter it, that threat will continue to grow as technology develops and criminals adapt. If we are to be successful in combating AI-generated fraud, we need to shift the AI advantage away from the criminals and towards those trying to protect consumers and honest businesses. Enforcers and industry need the same (or better) AI capabilities than the criminals to detect and disrupt their activities.

Prevention remains a critical defence against all fraud. Ensuring consumers understand how AI can make scams more convincing, and equipping them with clear, practical advice to protect themselves, will become ever more important as this technology develops.

REPORTING

Only an estimated 14% of fraud cases are reported in England and Wales, yet it is the most common crime. NTS and its partners encourage all victims to report fraud and scams in the following ways:

- To report concerns or get advice, contact the Citizens Advice Consumer Helpline on 0808 223 1133 (England and Wales)
- Use Report Fraud's online tool at www.reportfraud.police.uk or call Report Fraud on 0300 1232040
- In Scotland, contact Advice Direct Scotland on 0808 164 6000, or for Northern Ireland call Consumerline on 0300 1236262
- If a scam has just happened or you feel threatened or unsafe, call the Police