The Ultimate Guide to Scams in the UK, in 2025

BY JANE FRANKLAND MBE

As Seen on The Vanessa Feltz Show: What to Do if You're Targeted by a Scam

After joining Vanessa Feltz on Channel 5 to talk all things scams, in April 2025, I wanted to follow up with a clear guide for anyone who's ever been targeted — or worries they might be next.

Scams today aren't just dodgy emails or shady phone calls. Fraudsters use AI, social engineering, and emotional manipulation to steal not just money, but also trust, time, and peace of mind. And it's hitting home: £11.4 billion is lost to scams every year in the UK, with an average loss of £1,443 per person. Yet, 71% of victims never report it!

Let's change that.

The Ultimate Guide to Scams in the UK, in 2025

Fraudsters are blending cutting-edge tech with emotional manipulation to con even the most cautious. From AI-generated voices to realistic websites and stolen accounts, scams today are slick, fast, and global. But knowledge is power when used well— and here's how to protect yourself, your money, and your peace of mind.

Today's Most Common Scams

According to Ofcom, over half of all fraud cases in the UK involve impersonation scams — but other types are quickly gaining ground. Many exploit urgency, loss, and authority to trick victims into sharing personal info or making payments. Here's a breakdown of the most widespread and damaging scams today:

Impersonation Scams (51% of fraud cases) where fraudsters pose as: • Banks, HMRC, DVLA, or government agencies. • Couriers (e.g., Royal Mail, DHL, FedEx). • Tech support or utility companies. • Subscription services (e.g., Netflix, Amazon).	**Investment Scams** • Bogus crypto schemes, "get rich quick" plans, or fake stock tips. • Often promoted through fake celebrity endorsements. Martin Lewis, Elon Musk, or Jeremy Clarkson are some of the most popular.
Romance & Dating Scams • Over £400 million lost since 2020. • Victims are emotionally manipulated over weeks or months. • Scammers use fake personas often posing as military personnel or celebrities e.g., a French woman recently lost £700,000 to scammers pretending to be Brad Pitt using AI-generated photos and fake documents (BBC).	**Catfishing & Sextortion** • Fake online identities used to lure victims into romantic or sexual conversations. • Victims are then blackmailed with intimate content
Ticket & Holiday Scams • Fake tickets for concerts, sports events, or festivals. • Fake holiday rentals and too-good-to-be-true travel deals. • Over £10 million lost to ticket fraud alone last year.	**Job & Employment Scams** • Fake job listings or recruiters requesting upfront fees or personal data.
Health & Medical Scams • Fake treatments, supplements, or medical consultations — often targeting vulnerable people.	**Shopping Scams** • Fake online shops, social media ads, or marketplace listings. • Goods are never delivered — or are counterfeit.
QR Code & Quiz Scams • Scannable codes (e.g. in parking lots) redirect to malware ridden websites. • "Fun" quizzes used to gather personal data for fraud.	**Kidnapping & Ransom Scams** • Fake calls or messages claiming a loved one has been kidnapped. • Victims are pressured to pay a ransom urgently.

Also Emerging:

- Subscription Trap Scams: Hidden charges in free trial offers.
- Advance Fee Frauds: “Pay a fee to release your prize/funds”.
- Fake Charity Appeals: Especially after major disasters or global events.
- “Mum, I’ve lost my phone” Texts: Designed to exploit parental urgency.

How Scammers Exploit Emotion & Technology

Scammers rely on emotional manipulation and increasingly tech to catch people off guard — especially when we’re distracted, tired, or just trying to get through a busy day.

Emotional Triggers:

- Urgency and Fear: “Act now — or lose access, money, or an opportunity.” Urgency bypasses rational thinking.
- Guilt or Authority Pressure: Messages from “your boss,” “the bank,” or “your child” asking for urgent help or discretion.
- Greed and Hope: Fake investments, prize wins, or romance scams promise something too good to miss.

Technical Tactics:

- AI-Powered Fakes: Realistic cloned fake voices, images, and video calls, and AI-written emails mimicking real people like your boss, friends or family with alarming accuracy.
- MFA Fatigue Attacks: Bombarding you with login requests until you mistakenly approve one out of frustration or habit.
- MFA Bypass Methods: SIM swaps, malware, or phishing sites that trick you into revealing or approving access.
- Lookalike Domains & Interfaces: Scammers replicate login screens or domains so well that your browser or even you may not notice at first glance.
- Auto-fill Exploits: A small but critical sign – when your password manager doesn’t autofill — it might be a scam site. Always stop and check the URL.

Even cybersecurity experts get caught out, like Troy Hunt, creator of Have I Been Pwned (read his post).

He explained:

> *“There are moments that should raise red flags but don’t — like when your password manager doesn’t autofill. You might think, ‘Why didn’t I stop there?’ But it happens all the time.”*

Pro Tips:

- Pause if something feels off. Don't let urgency cloud your judgment.
- Check URLs carefully. Typos, extra characters, different fonts and domains are red flags.
- If autofill doesn't work, it might be because you're on a fake site.
- Don't approve unexpected MFA prompts. If in doubt, reject and investigate.

Upgrading Your Security Game

Use Strong Passwords and Managers

- Use a password manager to create and store unique, complex passwords.
- Make each password at least 12 characters long and use a mixture of lowercase and uppercase letters, numbers, and symbols.
- Alternatively, as advised by the UK National Cyber Security Centre (NCSC), use three random words to make your password e.g., paperhumbleconnect.
- Avoid reusing passwords across different services.
- If you're not into digital storage, write your passwords down and store them safely offline.

Enable Multi Factor Authentication (MFA)

MFA adds a layer of security, but not all methods offer the same protection:

- SMS codes can be intercepted or phished.
- App-based MFA (like Google Authenticator) is more secure, but still vulnerable to SIM swaps or malware.
- Passkeys are the gold standard — phishing-resistant, cryptographic credentials tied to your device. They're now supported by Apple, Google, and Microsoft.
- Bottom line: While some MFA methods are stronger than others, any MFA is better than none. If it's available — use it. And whenever possible, opt for passkeys.

Red Flags to Spot Scams Early

Urgency & Pressure Tactics

- Messages that pressure you to act immediately.
- Sudden "security alerts" prompting you to log in, reset your password, or take some other action.
- Being told to keep the interaction secret.
- Pressure to bypass normal security steps (e.g., turning off MFA).

Suspicious Payment Requests

- Being asked to send money in return for a bigger payout.
- Requests for gift cards, crypto, or wire transfers — these are untraceable.
- “Friends and Family” PayPal requests — this removes refund protection.

Impersonation & Fake Accounts

- Unfamiliar or spoofed sender addresses (e.g., amazon.uk-support@randomdomain.com).
- Emails or texts with poor grammar, odd phrasing, or strange links (less common due to AI).
- Avoidance of video calls or in-person meetings\Contradictory stories or evasive answers.

Online Clues & Website Issues

- Attachments and links.
- Unusual URLs or fake website clones — hover to check the real link.
- Login pages or forms on non-secure websites (look for “https://” and a padlock).
- Auto-fills not working in password managers like 1Password — may indicate a fake site.

Personal Information Requests

- Requests for personal or financial details.
- Requests for remote access to your device — legitimate services never do this unexpectedly.

What to Do if You’ve Been Targeted

Pause & Don’t Panic

- Take a breath. Don’t act on impulse.
- Talk it through with someone you trust — scammers rely on isolation and urgency.

Contact Your Bank Immediately

- Call 159, a call number that was set up by Stop Scams UK, and can’t be spoofed. This will safely connect with your bank’s fraud team.
- Also cancel any upcoming or recurring payments related to the scam.

Report the Scam

- Inform the legitimate company that was impersonated.
- Forward suspicious emails to report@phishing.gov.uk .
- Report the incident to Action Fraud (link below).

- If you're in immediate danger or the scam involves threats (e.g. kidnapping scams), call the police.

Monitor and Protect Your Accounts

- Change all passwords, especially for affected or related accounts.
- Enable muMFA, or passkeys, if they're supported.
- Use a password manager and avoid password reuse.
- Check if your email or phone has been exposed at HaveIBeenPwned.com.
- Monitor your credit score and consider placing a fraud alert or using CIFAS Protective Registration.
- Review your device security — ensure your software is up to date and scan for malware.

Increase Your Awareness and Get Support

- Get Safe Online – tips on secure browsing and fraud prevention.
- Stop Scams UK – advice and useful tools to prevent scams.
- Action Fraud – report and track cases.
- The Cyber Helpline – free expert guidance on cyber-related scams.
- Citizens Advice Scams Action – 1:1 help for scam victims.
- Victim Support – for emotional and practical support.

Pro Tips:

- Use Scam-Checking Tools like Ask Silver. Sign up, scan the QR code they'll send you which will open in WhatsApp and then Upload suspicious texts, emails, or websites for instant AI analysis.
- Check a Website enables you to verify if a website is legitimate before visiting.
- Check for rogue devices or logins: Look for unfamiliar devices on your email or cloud accounts (like Gmail, Apple, or Microsoft accounts).
- Preserve evidence: Take screenshots, keep messages, save bank details or emails that might be useful for investigations or future claims.

Can You Get Your Money Back?

- If the transaction was unauthorised, your bank must refund you, unless you were grossly negligent.
- If you authorised the payment —known as an Authorised Push Payment (APP) scam — it's trickier. But if your bank is signed up to the CRM Code, officially the Contingent Reimbursement Model Code, you might still get a refund if you acted reasonably.
- If they deny it:
    - Request a formal review
    - Escalate to the Financial Ombudsman

Scam Snapshot: The Latest

- £11.4 billion lost to scams annually in the UK
- £1,443 average loss per victim
- 61% of people face scams monthly
- 71% don't report them
- 53% of victims report mental distress
- Only 18% recover their money
- AI-powered scams are on the rise
- Most impacted age group: 35–44
- Largest losses: 55–64 demographic
- Women slightly more affected than men

A Scam-Free UK: What Needs to Happen

- Products and services that are secure by design and secure by default.
- More companies using Passkeys.
- Stricter accountability for social platforms and tech companies. (The Online Safety Act — active since March 2025 — is a step forward)
- Better public education on modern scam tactics, for all levels, and on platforms they frequently use. Finland embedded critical thinking, digital literacy, and resilience education right into their national curriculum in 2017 —from primary school upwards. They are now one of the most secure countries in the world.
- Easier and faster reporting tools.
- Stronger refund and support systems for victims.
- Cross-industry data sharing and tech collaboration.