



How to avoid romance scams

Over the last few weeks, I have been speaking publicly about the sharp rise in romance scams across the UK, including an interview with ITV Tyne-Tees News earlier this month.

While preparing for that interview, one thing stayed with me. Even working in technology, even living and breathing cyber risk every day, I had not fully appreciated just how vulnerable ordinary online interactions can be.

Romance scams are no longer a fringe issue or a niche form of fraud. They are one of the fastest-growing cyber crimes in the UK, and they rely far more on emotional manipulation than technical trickery.

A personal reflection

After many years of marriage, I spent a brief period exploring internet dating. It was not long, but it was enough to give me a sense of how much the landscape has changed.

Like many people, I assumed the main risks were the familiar ones. A bit of catfishing. Photos that did not quite match reality. Men exaggerating their height or other details, making me second-guess what I was really getting into. The occasional awkward conversation. Or the worry that a seemingly harmless date could turn dangerous.

What I did not fully consider at the time was the organised cyber crime operating behind the scenes. As I reviewed the latest figures while preparing for my interview, I was genuinely shocked:

- £106 million lost to romance fraud in the UK last year
- Reports increasing by around 20 percent year on year
- Average losses of more than £11,000 per victim
- AI-generated profiles making it harder than ever to tell what is real, with less than half of participants in a Norton study able to tell an AI image from a real one

This is not about people being naïve. It is about criminals becoming smarter, faster, and more emotionally sophisticated. They deliberately combine loneliness, connection, and technology into something deeply manipulative.

Why romance scams are surging

As they carry major financial repercussions for so many, these are life-altering financial attacks. We are currently witnessing a perfect storm created by three distinct factors:

- The loneliness epidemic and post-pandemic shifts have changed how we seek connection. Loneliness is a powerful psychological factor that hackers exploit to bypass our natural scepticism.
- As dating platforms hit their 30-year anniversary, they have become the primary way we meet people. This provides a target-rich environment for criminals.
- Generative AI tools like ChatGPT and Co-pilot allow scammers to generate believable, fluent, and emotionally resonant messages at scale.

What a romance scam typically involves

In the world of IT security, we often talk about the stages an attacker goes through to breach a system. A romance scam follows a similar, highly structured path:

1. Reconnaissance and baiting

Fraudsters don't just pick targets at random. They often mine social media for data, analysing interests, recent life changes (like a divorce or bereavement), and even your specific brand of humour. They then create a profile designed to be your 'perfect match'.

2. Moving off-platform

Most dating apps have security algorithms designed to detect scam patterns. To avoid detection, the attacker will quickly try to move you to encrypted or unmonitored services like WhatsApp.

3. Emotional grooming

This stage involves 'love bombing', where the scammer creates an intense, rapid emotional bond. Research shows that nearly 40% of victims are asked for money within the first month. By establishing a high-trust environment quickly, they disable your critical thinking.

4. The crisis

Once the bond is set, a crisis occurs. It's always urgent, highly emotional, and involves a request for funds. Common stories include medical emergencies, legal trouble, or travel costs to come and meet you.

The growing role of AI-generated profiles

One of the most worrying developments I am seeing is the rise of AI-generated profiles. Scammers now use realistic images of people who do not exist, making traditional checks like reverse-image searches less reliable.

Some even use deepfake audio or video to appear briefly on calls. Automated messaging tools allow them to respond instantly with tailored, romantic messages that feel personal and convincing. Profiles that appear overly polished, lack candid photos, or respond with near-instant messages should be treated with caution. Small inconsistencies often matter.

How to protect yourself

My advice is simple. Follow these simple rules and you'll be in a better position to know how to avoid romance scams this Valentine's Day and all year-round:

- **Slow down:** Scammers rely on speed and emotional pressure. If someone is declaring love within days or creating a sense of impending crisis, exercise restraint.
- **Verify via video:** Demand a real-time video call early on. If they consistently have bad Wi-Fi or a broken camera, they are hiding their identity.
- **Reverse-image search:** Use tools like Google Lens to see if their profile picture appears on stock photo sites or belongs to a different person entirely.
- **Keep it on the app:** Do not move to private messaging until you have met in person. Use the safety tools built into the platform.
- **Never send money:** No matter how heartbreaking the story, never send money, gift cards, or cryptocurrency to someone you haven't met.

Why talking about this matters

Technology creates incredible opportunities for connection, but it also creates opportunities for criminals. Nobody is immune to emotional manipulation when the timing and approach are right.

Romance scams thrive on shame, secrecy, and self-blame. Talking about them openly removes stigma and helps others recognise warning signs earlier. If you believe you or someone you care about may be affected, report the profile immediately and contact [Report Fraud](#) your bank if any money has been sent. Support is available.

At Net-Defence, we believe awareness is one of the strongest forms of protection. Staying cyber-aware matters not just at work, but in every part of our digital lives. Stay safe, stay aware, and keep the conversation going.