

Keep Your Money Safe



Surrey Police and Sussex Police Fraud Newsletter

In this issue:

Amazon scam warning

How to spot AI content online

AMAZON SCAM WARNING

Sussex and Surrey Police are witnessing an increase in cases where fraudsters are posing as working for Amazon, in order to access the victim's account or personal bank details.

One report stated that the victim had received a telephone call from someone claiming to be from Amazon, informing her of suspicious activity on her amazon account and there was an iPhone added to the basket. She then checked her account and could see the phones in the basket. They told her she had been hacked and asked her to share her screen and share her bank details. The fraudster took £900 from her accounts.

These individuals are calling victims, claiming that someone is purchasing expensive items on their Amazon account, and that they wanted to confirm it was them. When the victim states that it is not them making the purchase, the fraudster tells them this means that their account has been hacked and takes the victim through steps to "rectify" this, which usually involves them gaining remote access to their device.

Once they have remote access, they can access the victim's online banking and make transfers, often claiming that are moving their money to a "safe account" which is actually just an account belonging to the fraudster. They may also access the victim's Amazon account and place orders to themselves. This will often include the victim receiving a one-time passcode (OTP) to their phone and being requested to read this out to the fraudster so that they can gain access to their Amazon account.

“Each month we see many incidents of fraudsters targeting our residents in an attempt to defraud them. We're working hard to prevent this and support vulnerable victims of fraud or scams. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim.”

Detective Chief Inspector
Antony Leadbeatter
Surrey Police &
Sussex Police
Economic Crime Unit

Advice:

- If you receive an unexpected phone call and they ask you to download a remote access app, it will be a scam.
- Hang up and check your purchase history on your Amazon account for reassurance.
- If you are still unsure, contact Amazon through the genuine website or app.
- Never provide anyone with your one-time passcode (OTP)
- Do not be pressured – fraudsters will create a sense of urgency to convince victims to do what they are asking.
- Hang up the phone, give yourself time to think, and speak to a friend or family member about it.

How to spot AI content online

You've probably seen AI-generated clips on social media - or even convincing impersonations of celebrities, such as Martin Lewis. They might look professional at first glance, but you don't need to be a tech expert to protect yourself. Instead of hunting for one big mistake, get into the habit of slowing down and looking for several clues.

Just as you wouldn't buy a "designer" watch for £20 from someone in a car park, don't trust an image or video simply because it looks polished.

HOW TO SPOT AI FACES

Not perfect. But these red flags can help you notice the tells.



BLOCKY EYE SHADOWS

Shadows around the eyes can look blocky, patchy or unnatural instead of smooth and gradual.

Look for pixelated or blurry shadows under the eyes.



POOR LIP SYNC

Words and lip movements don't line up perfectly. Watch for delays, uneven shapes or missing mouth movements.



AWKWARD FACE MOVEMENTS

Expressions may look stiff, delayed or unnatural. Blinks can be too infrequent or uneven.



BLURRY HAIR

Hair often looks smudged, fuzzy or melts into the background. Strands may lack detail or consistency.



WAX/PLASTIC SKIN

Skin may look overly smooth, shiny or airbrushed. Pores, fine lines and natural texture are often missing.



INCONSISTENT AGE

Skin texture, eyes and facial features don't match. For example, smooth skin with wrinkled eyes or uneven signs of aging.



QUICK CHECKLIST



Does the face look overly smooth?



Do the eyes and shadows look off?



Do lip movements match the speech?



Do expressions and blinks feel natural?



Does the age and skin texture look consistent?

Visual clues that something may be AI-generated

AI-generated faces often contain tiny imperfections that our brains gloss over:

- Eyes and shadows may look blocky, blurred, or unnaturally sharp.
- Hair can appear soft, smudged, or melted into the background — AI struggles to render thousands of individual strands.
- Skin may look overly smooth, plastic, or airbrushed. Real skin has texture, pores, and subtle imperfections.
- Lip-sync issues are common in celebrity impersonations — the voice may sound flat or monotone, and the lips don't quite match the speech.
- Age inconsistencies such as youthful skin paired with older-looking eyes.

Protecting yourself from impersonation

Consider agreeing a simple AI safety word with close family or associates. If criminals impersonate someone you know, they won't know the word.

Whilst it's tempting to waste a scammer's time on the phone, it's safer to hang up immediately. Criminals can now record your voice and attempt to clone it — so the less audio you give them, the better.

Will AI become indistinguishable from reality?

People often ask whether AI will “take over” or become impossible to detect. Our answer is simple: look at the video game industry. Even with millions of pounds in investment, huge development teams, and years of work, we still aren't at a point where video games look truly indistinguishable from real life.

AI tools have only milliseconds to generate images and video — so we're not close to perfect realism yet.

The core message: NEVER ASSUME. ALWAYS VERIFY.

