A Tech Savvy AI Expert Nearly Got Scammed by AI. The Long Con Is Coming for You

Thursday 24 September, 2026

Most of us think we know what a scam call sounds like. Someone wants your bank details, your password, a security code or access to your account. There is usually urgency, pressure, a foreign accent and something that feels slightly wrong. But what happens when none of those warning signs are there?

That is exactly what happened recently to a tech savvy AI expert who came surprisingly close to being caught by a sophisticated scam. The first call was supposedly from the police. They explained that some of his information had been discovered during a criminal investigation and provided him with a crime reference number.

Naturally, he checked the telephone number on Google. It appeared legitimate, with several search results associating the number with the police department the caller claimed to represent. More importantly, the caller did not ask for anything. There was no request for a password, date of birth, bank details or money. They simply explained what had happened, gave some information and ended the call.

Later, another member of the supposed police team called. Again, nothing obviously suspicious. They talked through sensible precautions, discussed what he should keep an eye on and explained what might happen if some of his information had been compromised. The conversation was helpful, professional and reassuring.

Then came another call. This time the conversation moved towards cryptocurrency and how Bitcoin could potentially be compromised. They recommended installing a security application, and the application itself was completely genuine. There was still no obvious reason to be concerned.

The scam only became apparent when the caller suggested a quicker way to install the software. Rather than finding the application through the normal official route, they suggested going to a particular website and downloading it from there. That website was the real scam. It contained a fake version of the application designed to give the criminals access to cryptocurrency.

Fortunately, something about the domain name did not look right. It used an unusual domain extension rather than the familiar address he expected. While still on the telephone, he checked the website independently on his computer and Chrome also raised concerns about the site. He stopped before downloading anything, but he had come far closer to being caught than many technically experienced people would like to admit.

What makes this attack important is not simply the fake website. It is everything that happened before it.

Traditional scammers have always had one major problem: time costs money. If a human scammer spends hours speaking to someone who never hands over any money, those hours have been wasted. That naturally encouraged criminals to push victims quickly, create urgency and move on if the scam was not working.

AI changes that equation. An AI driven system can manage large numbers of conversations at the same time. It does not get tired, lose patience or care whether a scam takes one telephone call or ten. It can remember previous conversations, keep the story consistent and slowly build credibility over days or weeks or months before the victim is ever asked to do anything.

That means the first telephone call no longer needs to contain the scam. Its only purpose may be to establish trust. The second call can reinforce the story. The third can provide useful advice. Only much later does the real request appear, by which point the person on the other end of the phone no longer feels like a stranger.

There is another element that makes this kind of fraud more convincing: criminals can also influence what you find when you try to check them.

Searching a telephone number on Google can still be useful, but it should not be treated as proof that the caller is genuine. Criminals can rapidly create multiple fake websites using AI, containing the telephone number, organisation name and other details they want people to find. They can also compromise

Media:



Related Sectors:

Business & Finance :: Computing & Telecoms ::

Related Keywords:

Ai :: Lon Con :: Criminals ::

Scan Me:

legitimate websites and insert pages containing carefully chosen keywords, a technique often referred to as SEO poisoning.

The aim is simple. If someone receives a call claiming to be from a particular police department and then searches the number, the scammers want the search results to confirm the story.

Voice cloning adds another serious risk. The caller may not even sound like a stranger. AI can be used to reproduce the voice of a colleague, managing director, friend or family member using previous phone calls. This means recognising someone's voice can no longer be treated as reliable authentication.

The most important defence is therefore to verify people outside the conversation they have started. If someone claims to be from the police, end the call and contact the police independently using a number you find yourself. If your bank calls, use the number on your bank card or official website. If a colleague asks you to transfer money, verify the request using another established company process, consider have a "safe word" you use when verifying payments. If someone recommends software, find the official website or app store yourself rather than using the link they provide.

The worrying thing about the next generation of scams is not simply that AI can create convincing voices or fake websites. It is that AI gives criminals something they have never had at scale before: almost unlimited patience.

The scam does not have to happen on the first call. The first call can simply make you trust the second, the second can make you trust the third, and by the time the real request finally comes, you may no longer believe you are talking to a stranger.

That is what makes the AI powered long con so dangerous.

By Juliet Moran

Technical Director

https://telephonesystems.cloud

Company Contact:

Hosting Systems Ltd

T. 01782 608608
E. juliet@systems.co.uk
W. https://systems.co.uk

View Online

Additional Assets:
https://telephonesystems.cloud

Newsroom: Visit our Newsroom for all the latest stories:
https://www.systems.pressat.co.uk