# Cybersecurity experts warn of rise in AI impersonation scams and urge use of secret passwords



As advancements in artificial intelligence continue to reshape various sectors, their implications for personal security have become increasingly concerning. In recent discussions surrounding the rise of sophisticated AI impersonation scams, cybersecurity experts have issued urgent warnings and advice on protective measures that individuals can take to safeguard their identities.

Cody Barrow, the chief executive of the cybersecurity firm EclecticIQ and a former advisor to the US government, emphasises the urgency of the situation. He notes the alarming ease with which cybercriminals can now create realistic deepfakes, leveraging readily available AI technology. Speaking candidly, Barrow highlights the unsettling reality that “AI is huge. It’s not just hype.” With a heightened risk of impersonation scams, he advocates for establishing secret passwords or phrases amongst friends and family. This relatively simple measure can serve as a crucial verification tool when facing potential AI-generated communication, especially in situations involving requests for money or personal assistance.

Barrow's insights resonate within a broader context of rising data breaches and cyberattacks. Recent incidents affecting prominent UK retailers, such as Marks and Spencer, have illustrated vulnerabilities that can be exploited through human error. Marks and Spencer reported that their breach was a result of social engineering tactics that took advantage of third-party access. According to Barrow, hackers often capitalise on predictable security setups, such as standard two-factor authentication, making it easier to manipulate unsuspecting individuals into compliance.

Further recommendations from cybersecurity experts reinforce Barrow's message. Research underscores the importance of establishing a family safe word to enhance identity verification when unexpected circumstances arise. This suggestion is echoed across multiple platforms, including advice from organisations like CSIRO and Seacoast Bank. In the face of evolving cyber threats, maintaining a heightened awareness of personal information shared online and regularly updating security measures is essential.

As the landscape of digital communication evolves, the tactics employed by scammers are becoming increasingly sophisticated, with AI-enabled voice cloning services used to replicate unsuspecting individuals’ voices. This has raised alarm, suggesting that even the most cautious individuals can be caught off guard. A simple yet effective strategy—creating and utilising a shared secret word—can provide an additional safeguard, allowing people to confirm their identities in potentially compromising situations.

The situation calls for not only personal vigilance but also a collective effort to enhance cybersecurity measures across the board. As noted by insights from various cybersecurity experts, many individuals may not realise that they have previously been victims of data breaches, leaving them susceptible to future scams. Given the statistics indicating that a significant proportion of the population have had their personal information compromised at some stage, implementing these straightforward yet powerful practices can help mitigate the ongoing risks associated with AI-driven fraud.

In the face of rapidly changing technology and its implications, it is more important than ever for both young and older individuals—who may possess varying levels of digital savvy—to remain informed and proactive about their online security.

## Reference Map:

* Paragraph 1 – [[1]](https://www.independent.co.uk/news/uk/home-news/ai-scam-password-warning-uk-b2757694.html), [[4]](https://www.scientificamerican.com/article/a-safe-word-can-protect-against-ai-impostor-scams/)
* Paragraph 2 – [[1]](https://www.independent.co.uk/news/uk/home-news/ai-scam-password-warning-uk-b2757694.html), [[3]](https://corporate.visa.com/en/sites/visa-perspectives/security-trust/executive-impersonation-scams.html)
* Paragraph 3 – [[2]](https://www.csiro.au/en/news/all/articles/2024/december/cybersecurity-top-tips), [[5]](https://www.seacoastbank.com/resource-center/blog/ai-a-new-tool-for-scammers), [[6]](https://www.keepersecurity.com/blog/2023/06/21/how-cybercriminals-are-using-ai-for-cyberattacks/)
* Paragraph 4 – [[5]](https://www.seacoastbank.com/resource-center/blog/ai-a-new-tool-for-scammers), [[7]](https://nationalcybersecurity.com/ai-hacking-scams-are-on-the-rise-heres-how-to-protect-your-money-points-and-miles-hacking-cybersecurity-infosec-comptia-pentest-hacker/)
* Paragraph 5 – [[1]](https://www.independent.co.uk/news/uk/home-news/ai-scam-password-warning-uk-b2757694.html), [[4]](https://www.scientificamerican.com/article/a-safe-word-can-protect-against-ai-impostor-scams/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.independent.co.uk/news/uk/home-news/ai-scam-password-warning-uk-b2757694.html> - Please view link - unable to able to access data
2. <https://www.csiro.au/en/news/all/articles/2024/december/cybersecurity-top-tips> - This article from CSIRO provides five cybersecurity tips to protect against scams and deepfakes. It emphasizes the importance of having a family safe word to verify identities, advises not to hesitate in hanging up on suspicious calls, recommends enabling multi-factor authentication, suggests turning on banking push notifications, and highlights the need to be aware of personal information shared online. These measures aim to enhance personal security in the face of evolving cyber threats.
3. <https://corporate.visa.com/en/sites/visa-perspectives/security-trust/executive-impersonation-scams.html> - Visa's article discusses the rise of executive impersonation scams facilitated by AI-generated deepfakes. It offers top tips to avoid such scams, including being skeptical of unusual communications, verifying identities through official channels, avoiding clicking on unknown links, securing sensitive data with strong passwords and multi-factor authentication, reporting suspicious activity, and staying informed about emerging threats. The piece underscores the importance of vigilance and proactive measures in cybersecurity.
4. <https://www.scientificamerican.com/article/a-safe-word-can-protect-against-ai-impostor-scams/> - This Scientific American article highlights the increasing use of AI voice-cloning services in impostor scams. It recommends establishing a safe word with family and friends to verify identities during unexpected communications, especially when requests for money are involved. The piece emphasizes the effectiveness of this simple yet powerful strategy in preventing AI-infused phone scams and protecting personal and financial information.
5. <https://www.seacoastbank.com/resource-center/blog/ai-a-new-tool-for-scammers> - Seacoast Bank's blog post discusses how scammers are leveraging AI to replicate voices and deceive individuals. It provides protective measures such as creating a safeword with family and friends to authenticate phone calls, strengthening passwords with two-factor authentication, and allowing unknown calls to go to voicemail to verify identity. These strategies aim to safeguard personal information from AI-driven scams.
6. <https://www.keepersecurity.com/blog/2023/06/21/how-cybercriminals-are-using-ai-for-cyberattacks/> - This Keeper Security blog post explores how cybercriminals are utilizing AI for cyberattacks. It offers guidance on staying safe from AI-enabled cyberattacks, including securing accounts with strong, unique passwords and multi-factor authentication, regularly backing up data, keeping software and devices up to date, and creating a safe word with family to prevent AI vishing scams. The article emphasizes proactive measures to enhance cybersecurity.
7. <https://nationalcybersecurity.com/ai-hacking-scams-are-on-the-rise-heres-how-to-protect-your-money-points-and-miles-hacking-cybersecurity-infosec-comptia-pentest-hacker/> - This article discusses the rise of AI hacking scams and offers protection strategies. It advises having a family verification method, such as a secret family password, to confirm identities during unexpected communications. The piece also recommends setting up two-factor authentication on accounts and considering the use of passkeys for secure digital verification. These measures aim to protect personal and financial information from AI-driven scams.