# Cybersecurity expert reveals simple secret code to thwart deepfake scams



Amid an escalating wave of impersonation scams fed by advanced deepfake technology, the public faces an overwhelming challenge in keeping cyber criminals at bay. However, a simple, proactive strategy proposed by security expert Cody Barrow offers a glimmer of hope. The solution? A secret password shared among family and friends designed specifically to help them discern whether they are truly communicating with a loved one or an AI-generated deepfake.

Deepfake technology, which manipulates audio and video to create convincingly realistic impersonations, has become alarmingly accessible. Barrow, who leads the cybersecurity firm EclecticIQ, observes that the advancements in artificial intelligence have significantly lowered the barriers for scammers. He warns that, as the digital landscape evolves, individuals must adopt stronger safeguards beyond traditional online security measures. “AI is huge. It’s not just hype,” he noted. His personal anecdote—utilising a unique code with his wife for verification—underscores the necessity of this approach in an age when deepfake scams are surging.

These impersonation scams are not merely theoretical. High-profile individuals, including financial commentators and corporate executives, have already experienced fraudulent uses of their likenesses in various scams, leading to substantial financial losses. For instance, a notable case involved a UK firm conned out of $25 million through a deepfake impersonation of a corporate leader. Such incidents highlight a troubling trend in which scammers exploit generative AI technology to create increasingly sophisticated and convincing deceptions.

The rise in deepfake scams coincides with a broader surge in cyberattacks across industries. Retailers such as M&S and the Co-op have faced recent data breaches, prompting calls for enhanced security measures. The repercussions of these breaches often extend beyond immediate financial loss; they can erode public trust and lead to long-term brand damage. In acknowledging this reality, experts emphasise the importance of educating users about warning signs, such as discrepancies in video authenticity, including unnatural movements or inconsistent voice tones.

Moreover, enterprises are urged to adopt multi-layered security protocols as part of their response strategy. This includes recommendations for robust communication practices, such as callback verification for financial requests and investment in AI detection tools to identify manipulated media. As a safeguard against scams that have increasingly targeted sensitive information—especially during tax season—individuals are advised to verify requests through independent means and exercise caution with unsolicited communications.

The UK's recent Online Safety Act also reflects a growing awareness of the need for stricter regulations. This legislation mandates quicker removal of illegal material and aims to hold social media companies accountable for moderating harmful content effectively. Critics have argued, however, that current measures remain inadequate, underscoring the importance of user vigilance.

As the technological landscape continues to advance, cybersecurity will remain an evolving challenge. The proactive strategies put forth by experts like Barrow serve as crucial reminders that while deepfake technology poses significant risks, informed and engaged individuals can take steps to mitigate their vulnerability. Protecting oneself from these threats requires a blend of awareness, education, and the implementation of secure communications, enabling individuals and organisations to better navigate an increasingly complex digital world.

## Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/news/article-14748769/simple-trick-beat-deepfake-scammers-impersonating-stealing-cash.html?ns_mchannel=rss&ns_campaign=1490&ito=1490)
* Paragraph 2 – [[1]](https://www.dailymail.co.uk/news/article-14748769/simple-trick-beat-deepfake-scammers-impersonating-stealing-cash.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.ft.com/content/fcbdc88f-bbfd-4338-915a-9ef7970b2123)
* Paragraph 3 – [[3]](https://www.tomsguide.com/computing/online-security/ai-powered-tax-scams-are-here-how-to-stay-safe-from-deepfakes-phishing-and-more-this-tax-season), [[4]](https://www.reuters.com/legal/legalindustry/real-insurance-coverage-increasing-ai-deepfake-risks-2024-04-11/)
* Paragraph 4 – [[5]](https://apnews.com/article/879a6c2ca816c71d9af52a101dedb7ff), [[6]](https://www.netgainit.com/blogs/rise-of-ai-scams/)
* Paragraph 5 – [[2]](https://www.ft.com/content/fcbdc88f-bbfd-4338-915a-9ef7970b2123), [[7]](https://secutoris.com/news/the-rising-risk-of-deepfake-phishing-attacks)

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

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14748769/simple-trick-beat-deepfake-scammers-impersonating-stealing-cash.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.ft.com/content/fcbdc88f-bbfd-4338-915a-9ef7970b2123> - Deepfake scams are rapidly growing due to the accessibility and sophistication of generative AI technology, which enables scammers to create highly convincing fake videos impersonating public figures. Financial Times' commentator Martin Wolf and Money Saving Expert’s Martin Lewis are among many whose images and voices have been fraudulently used to promote fake investment schemes on social media platforms like Instagram and WhatsApp. Deepfakes are also being used in video calls to impersonate corporate executives, leading to significant financial losses, such as a $25 million scam involving UK firm Arup. Experts warn that many social media users are unaware of the capabilities of AI, making them more susceptible to these scams. Social media companies like Meta claim to combat this content using facial recognition and AI tools but have faced criticism for inadequate content moderation and slow response. The UK's new Online Safety Act requires quicker removal of illegal material. To avoid falling victim, users are advised to critically assess video authenticity by examining mouth movements, skin texture, eye behavior, and voice tone. It's crucial to report impersonations and alert others to prevent further spread of scams.
3. <https://www.tomsguide.com/computing/online-security/ai-powered-tax-scams-are-here-how-to-stay-safe-from-deepfakes-phishing-and-more-this-tax-season> - With the advance of AI technology, tax season brings an array of new scams involving deepfakes, phishing, and other fraudulent activities. Common schemes include W2 phishing scams, in which AI-generated calls, chatbot messages, or emails impersonate coworkers or executives to solicit sensitive tax information. Disaster Relief Fund scams capitalize on people affected by disasters, using fake donation sites to steal money or data. Offer in Compromise scams pose as debt relief options with false promises to settle tax debt. To stay safe, individuals should verify any requests for tax information through independent methods, be cautious of unexpected communications, and avoid sharing personal details online. The IRS offers an Identity Protection PIN to safeguard against unauthorized tax filings. Additionally, using VPNs, password managers, and updated antivirus software can provide extra security. Always remember, the IRS will not request personal information over phone calls or texts since they already have this data.
4. <https://www.reuters.com/legal/legalindustry/real-insurance-coverage-increasing-ai-deepfake-risks-2024-04-11/> - Cyber risks, especially those posed by deepfakes, are increasingly sophisticated and a major concern for corporate leaders. Deepfakes use AI to create realistic but false representations, such as altering facial features or mimicking voices, leading to scams that can result in significant financial loss. A notable example involves a Hong Kong company where deepfake technology was used to simulate a video conference, tricking an employee into transferring over $25 million to criminals. Companies should adopt measures to minimize these risks, such as implementing verification procedures and acquiring comprehensive insurance coverage. Traditional commercial crime policies, which offer coverage for social engineering scams, often feature sublimits, while cyber insurance provides higher liability limits and more extensive coverage for cyber risks like phishing and ransomware attacks. Insurers now demand better security protocols and may offer new endorsements to cover AI-related incidents. Regular consultation with professionals and continual evaluation of insurance policies are advised to ensure adequate protection against evolving cyber threats.
5. <https://apnews.com/article/879a6c2ca816c71d9af52a101dedb7ff> - An advanced deepfake operation targeted Senator Ben Cardin in a sophisticated attempt to deceive him into revealing sensitive political information. The attack involved a convincing video call with an AI-generated impersonation of Dmytro Kuleba, posing realistic visual and audio characteristics. The deception was noted only after the fake Kuleba asked leading, politically charged questions. This incident, involving AI technology, reflects an emerging trend in using sophisticated AI-backed schemes for fraud, political mischief, and misinformation. Experts highlight that recent technological advances have made such operations more accessible and impactful, foreseeing more of these incidents across various sectors. The incident has led to calls for heightened vigilance and authentication in political communications.
6. <https://www.netgainit.com/blogs/rise-of-ai-scams/> - Deepfake scams are becoming increasingly prevalent, leveraging AI technology to create convincing fake videos and audio that impersonate individuals. To combat these threats, experts recommend several strategies: implementing multi-factor authentication (MFA) for sensitive transactions, using callback verification procedures to confirm requests, investing in AI-powered detection tools to identify manipulated media, enhancing employee training to recognize deepfakes, and establishing robust communication policies that include clear protocols for handling requests. These measures aim to strengthen defenses against deepfake scams and protect individuals and organizations from potential harm.
7. <https://secutoris.com/news/the-rising-risk-of-deepfake-phishing-attacks> - Deepfake phishing attacks are on the rise, posing significant risks to businesses and individuals. To protect against these threats, it's crucial to implement proactive security measures. Key strategies include educating employees on recognizing deepfake phishing attempts, implementing multi-factor authentication (MFA) for critical systems, establishing verification protocols for high-risk requests, investing in AI detection tools to identify manipulated media, securing digital footprints by limiting personal and corporate data online, and strengthening incident response plans to address deepfake phishing attacks promptly. These measures can help mitigate the risks associated with deepfake phishing and enhance overall cybersecurity posture.