# AI-powered scams surge with deepfakes and voice cloning targeting older victims



The rapid evolution of artificial intelligence (AI) has provided scammers with unprecedented tools for deception, broadening the potential for fraud with alarming efficacy. From generating convincing fake messages and images to mimicking voices and crafting deepfake videos, AI empowers opportunistic criminals, making traditional safeguards seem inadequate in the face of increasingly sophisticated scams.

AI scams encompass a wide range of fraudulent activities where technology creates highly convincing content, from text messages to audio and visual impersonations. These tools, readily available online for legitimate purposes, have inadvertently facilitated a surge in scams that can be difficult for the average person to detect. Simon Miller, director of policy, strategy and communications at the fraud prevention service Cifas, points out that the speed at which criminals can utilise AI to devise fake documents and impersonate trusted individuals poses a significant threat. Particularly vulnerable are older individuals who, as highlighted by Miller, may lose years of savings in a single scam.

Romance scams are one of the most prevalent ways scammers exploit AI capabilities. Fraudsters create fictitious profiles on dating websites and social media platforms, employing AI-generated messaging and realistic audio or video communications to develop emotional connections with victims. A report from Barclays indicates a 20% increase in romance scams in early 2025, with victims averaging losses of £8,000. Alarmingly, those aged 61 and above are disproportionately affected, with average losses nearing £19,000. Kirsty Adams, a fraud expert at Barclays, stresses the importance of vigilance, urging users to trust their instincts when interactions feel overly solicitous or fast-paced. Victims are encouraged to communicate through the original platform and consult trusted friends or family before sending any money.

The rise of deepfake technology represents another facet of AI scams that warrants scrutiny. With the ability to produce highly accurate videos of people saying things they have not actually said, deepfakes are often leveraged to promote fraudulent investment schemes. A notable example involved a cloned video of financial expert Martin Lewis, which was circulated to entice viewers into purchasing fake investment opportunities. Jenny Ross, editor of Which? Money, cautions that while many deepfakes can appear alarmingly lifelike, certain indicators—such as misalignments in lip sync and unnatural movements—can alert viewers to their inauthenticity.

Voice cloning scams have also emerged as a growing threat, where scammers can replicate a person's voice from mere snippets of audio, such as voicemails or social posts. As a result, they can easily impersonate loved ones or officials demanding urgent financial assistance. The FBI has raised alarms about the use of these technologies to replicate the voices of high-profile figures, demonstrating how advanced AI influences not only everyday scams but also larger potential threats posed by cybercriminals. These impersonations become particularly insidious in times of sudden crises when individuals are more inclined to respond without verification.

Meanwhile, the UK’s Investment Association reported a staggering 57% surge in cloning scams in 2024. Fraudsters frequently impersonate legitimate investment firms, leading to substantial financial losses, with £2.7 million reported just in the second half of the year. Adrian Hood from the IA warns that the growing sophistication of these scams indicates a critical need for consumer vigilance. Despite fluctuations in overall fraud losses—showing a 29% decline across various categories—the rising numbers of impersonation incidents highlight a pressing need for consumers to authenticate investments through reliable channels.

In response to this burgeoning landscape of AI-facilitated fraud, individuals must adopt a cautious and informed approach to communications. Staying updated on the latest AI scam trends is vital, as is establishing multi-factor authentication on important accounts for added security. It is also crucial to verify urgent money requests through known contacts and official channels, rather than responding directly to unsolicited communications. Social media users should safeguard their accounts by setting privacy settings and being judicious about personal information shared online.

Understanding the nuances of AI technology is imperative in our digital age, especially as scammers become increasingly adept at exploiting these capabilities. Experts advise critical assessment of video authenticity and caution against the allure of too-good-to-be-true offers. In an environment where the line between genuine interaction and deception blurs, vigilance, education, and proactive security measures are key to safeguarding personal and financial information against the wave of AI-driven scams.

### Reference Map

1. Paragraphs 1, 2
2. Paragraph 3
3. Paragraph 4
4. Paragraph 5
5. Paragraph 6
6. Paragraph 7
7. Paragraph 8

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

## Bibliography

1. <https://www.saga.co.uk/money-news/how-to-avoid-ai-scams> - Please view link - unable to able to access data
2. <https://www.ft.com/content/4aea4a81-10d5-48f2-8594-8883a298363f> - Cloning scams surged by 57% in 2024, prompting the UK’s Investment Association (IA) to urge consumers to stay vigilant. Fraudsters impersonate legitimate investment firms by replicating websites, emails, or creating fake communication groups to deceive victims into transferring funds. In the latter half of 2024, 478 impersonation incidents were reported, leading to £2.7 million in losses, with nearly one in four attempts being successful. A total of 1,014 cloning scams were detected across the year. Adrian Hood from the IA warned that criminals are leveraging advanced tools, including artificial intelligence (AI), to increase the sophistication of these scams. While cloning scams are on the rise, overall fraud losses dropped by 29% between the first and second halves of 2024, totaling £5.4 million. Other types of fraud, like account takeovers and card fraud, also declined. Authorities recommend verifying firms using the Financial Conduct Authority’s register and reporting fraud to the Action Fraud center. £1.7 million in losses were recovered, highlighting some success in ongoing anti-fraud efforts.
3. <https://www.tomsguide.com/computing/online-security/how-to-spot-a-fake-chatgpt-site> - As interest in AI surges, numerous fake ChatGPT websites have emerged, mimicking OpenAI’s branding and user interface to deceive users. These sites, such as chat.chatbotapp.ai and hotbot.com, claim to use models like GPT-3.5 or GPT-4, but are not officially affiliated with OpenAI. While some employ OpenAI’s API, their lack of transparency, ad-heavy interfaces, vague privacy policies, and misleading claims pose risks to user data and device security. Common issues include personal data being logged, sold, or used to train other models, as well as malware threats from deceptive ads and pop-ups. The article reviews five fake AI platforms, highlighting usability but raising concerns about privacy, authenticity, and quality. Users are advised to stick with trusted platforms like ChatGPT, Gemini, Claude, or Perplexity, which offer free access to top-tier models with secure data practices. The key takeaway: avoid unofficial AI sites that may compromise your data under the guise of convenience and free access.
4. <https://www.axios.com/2025/05/15/artificial-intelligence-voice-scams-government-officials> - The FBI has issued a warning that scammers are increasingly using artificial intelligence (AI) to impersonate senior U.S. officials by mimicking their voices. This trend highlights the growing sophistication of cybercriminals in leveraging AI tools to exploit individuals. With just a few seconds of audio, AI technologies can generate highly realistic voice clones that are nearly indistinguishable from the actual voices, making these schemes particularly deceptive. The situation is exacerbated by recent federal layoffs, which have opened up new opportunities for cyberattacks by both criminal organizations and nation-state actors. Experts note that the ease and accessibility of voice cloning technology underscore the current reality of deepfake threats, emphasizing the urgent need for regulatory and technological safeguards.
5. <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.
6. <https://www.helpnetsecurity.com/2025/03/11/how-to-spot-ai-generated-scams/> - AI-generated scams are becoming increasingly sophisticated, making it challenging for individuals to detect fraudulent activities. To protect oneself, it's essential to approach unsolicited communications with caution, especially those that are urgent or offer something too good to be true. Staying informed about the latest trends in AI scams, such as deepfake videos and voice cloning, can aid in recognizing suspicious activities. Implementing multi-factor authentication (MFA) on all important accounts adds an additional layer of protection. Utilizing AI-detection tools can help identify AI-generated content, whether it's text, images, or videos. Verifying any urgent requests for money or sensitive information by contacting the person directly through verified phone numbers or emails is crucial. Despite the advancements in AI, adversaries' use of generative AI has not yet matched the hype, and by taking swift action, organizations and institutions can implement defenses to mitigate most AI-powered attacks.
7. <https://www.npr.org/2024/12/24/nx-s1-5235265/how-to-protect-yourself-from-holiday-ai-scams> - As AI technology advances, scammers are increasingly using it to create convincing fraudulent communications. To protect oneself, it's important to lock down social media accounts by setting them to private and limiting the personal information shared publicly. Carefully checking the web address before inputting any sensitive information is crucial, as scammers can use AI to create fake websites that seem legitimate. Always ensure the website is encrypted and the domain is spelled correctly. If in doubt, look up the age of the site using domain lookup databases. Additionally, be cautious of unsolicited communications and verify their authenticity through official channels.