# Experts warn of rising AI-powered healthcare scams targeting consumers



Amid growing concerns about the increasing use of artificial intelligence (AI) in fraudulent activities, experts are raising alarms about the rise of AI-powered scams targeting consumers, particularly in the healthcare sector. These scams, which have become more prominent in recent months, are causing financial and personal information losses, with experts predicting that 2025 may see a significant surge in such criminal activity.

The Better Business Bureau issued a warning back in March, alerting consumers to the dangers posed by AI scams designed to steal money and sensitive data. Reporting by Forbes also highlights expectations that 2025 could become a critical year when financial technology systems and bank accounts come under intensified attack by AI-enabled fraudsters.

Healthcare billing is one major area where AI is being exploited. Criminals are deploying sophisticated methods to send out fake medical bills and emails containing malicious links that aim to compromise personal information. AI's ability to fabricate convincing logos, images, and even videos makes these scams harder to detect. Scott Speranza, CEO of cybersecurity firm HealthLock, explained how AI's realism in creating fraudulent content can fool consumers. “AI can create images, videos and other content that’s so realistic it can be impossible to detect a flaw unless you zoom in on one small pixel that’s incorrect,” he said, speaking to AOL.com. Speranza further emphasised, “Never pay a bill without verifying its authenticity. Contact your insurance or healthcare provider via phone and ask if they sent you a bill.”

Consumers are urged to scrutinise any suspicious bills carefully. If charges are not recognised, contacting the healthcare provider directly using contact information from official websites—not from the questionable bill—is recommended. This precaution helps ensure that payers are dealing with legitimate sources before releasing funds.

Additionally, caution is advised against clicking on links or replying to unexpected emails or text messages purporting to be from insurance companies or healthcare providers. Speranza advised, “If you don’t regularly receive bills from your insurance company or healthcare provider via email, then don’t click on any links or reply to an email if you suddenly receive one. The same goes for text messages.”

Another practical recommendation to protect oneself is to pay bills using a credit card rather than a bank account or cash apps. Credit cards offer the advantage of enabling consumers to dispute inaccurate charges more easily, providing an additional layer of financial defence.

As AI technology continues to evolve and become more accessible, these scams are expected to grow in sophistication. Increased vigilance and careful verification are key strategies advised by experts to help consumers guard against becoming victims of AI-driven fraud.

The details and advice noted here were reported by AOL.com, referencing insights from industry experts and consumer protection organisations.

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

## Bibliography

1. <https://www.carltonfields.com/insights/publications/2024/hhs-warns-health-care-sector-of-ai-driven-phishing-social-engineering-attacks-on-it-help-desks> - This article discusses the Department of Health and Human Services' warning about AI-driven phishing and social engineering attacks targeting healthcare IT help desks, highlighting the increasing use of AI in fraudulent activities within the healthcare sector.
2. <https://arxiv.org/abs/2410.00434> - This study investigates deceptive patterns in social robots integrated with Large Language Models (LLMs) in healthcare, raising ethical concerns about AI's role in creating convincing but fraudulent content.
3. <https://www.govinfosecurity.com/feds-warn-healthcare-sector-ai-augmented-phishing-threats-a-23419> - This article reports on federal authorities warning the healthcare sector about AI-augmented phishing threats, emphasizing the rise of AI-powered scams targeting consumers, particularly in the healthcare sector.
4. <https://arxiv.org/abs/2504.03759> - This research highlights emerging cyber attack risks of medical AI agents, including vulnerabilities to adversarial prompts that can inject false information, manipulate recommendations, and steal sensitive data, underscoring the potential for AI to be exploited in fraudulent activities.
5. <https://www.helpnetsecurity.com/2024/08/23/fraud-tactics-ai-scams/> - This article discusses the growing prevalence of AI scams, including AI-generated voice-cloning technology used to impersonate individuals and organizations, leading to financial and personal information losses.
6. <https://www.bbb.org/all/scamstudies/phishing_scams_study/full-2024-phishing_scams-study> - This study by the Better Business Bureau reports a significant increase in phishing scams, with AI and text-based scams contributing to the rise, highlighting the dangers posed by AI scams designed to steal money and sensitive data.
7. <https://news.google.com/rss/articles/CBMiakFVX3lxTFBYQTktVnRRZkY4R2JGcm0yTzFrVkQwVVk5d3E4cHA4SWFtTW5pT2N2MUdYVTdDYl9QaTdNa3M3b1p3SG9mU1Eta053WGRNRGlTaDJNaUZTZkdCVnp1bVdYa3JIR3hYZ1dQTEE?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data