# Cybercriminals harness AI to launch unprecedented phishing and deepfake attacks



The cybersecurity landscape is undergoing a seismic transformation as artificial intelligence (AI) tools become increasingly accessible, empowering cybercriminals to launch sophisticated deception, infiltration, and disruption campaigns. This evolution poses significant challenges for both businesses and individuals, as traditional defence measures struggle to keep pace with the evolving tactics employed by attackers.

A noticeable shift in the nature of cyber threats has been documented, with AI facilitating an alarming increase in phishing and social engineering attacks. Recent findings suggest that phishing campaigns have surged dramatically, with a staggering 197% rise in email-based attacks reported in late 2024 alone. A vast majority of these assaults—over 40%—are now attributed to AI-generated content, marking a substantial leap in the sophistication of such operations. Whereas previous phishing attempts were often riddled with typographical errors, modern AI-driven emails can craft messages that mirror corporate communication styles precisely, incorporating stolen personal information and dynamically adjusting their content based on recipient interactions. According to a report by Cofense, a malicious email is now detected every 42 seconds, with AI-generated emails being particularly adept at bypassing conventional security measures.

The implications are dire. As highlighted in a recent FBI report, the state of Indiana experienced a dramatic 113% rise in internet crime complaints in 2024, reaching over 23,000 reports. While the overall financial losses declined from the previous year, the persistence of AI in amplifying fraud tactics—such as using voice and video AI tools for impersonation—has heightened concerns regarding the vulnerabilities, especially among older populations, who accounted for over $37 million in losses.

Deepfake technology further complicates the cybersecurity landscape by enabling multimodal deception. Cybercriminals have begun leveraging AI-generated audio and video to simulate authoritative voices, resulting in significant financial losses for corporations. For instance, a notable case involved a U.K. energy firm duped into transferring $243,000 following a call from what was believed to be their CEO, whose voice had been convincingly cloned. According to global surveys, nearly half of businesses have encountered video deepfake scams, reflecting a profound evolution in how cyber threats are executed.

Adding to the complexity, cybercriminals are increasingly deploying AI to enhance their malware. Tools are now capable of generating polymorphic malware that can dynamically change its code structure while maintaining harmful functionality. A ransomware report revealed that groups like RansomHub are utilising AI to optimise their encryption patterns and improve the effectiveness of their attacks. In a notable trend, these malicious algorithms have begun engaging in "zero-day hunting" on a scale previously unimaginable, leading to a significant uptick in exploitation attempts across critical infrastructure, particularly in North America.

This technological arms race highlights a troubling skills gap in the cybersecurity workforce. A report indicated that a significant proportion of enterprises—33%—lack staff capable of effectively addressing AI-driven threats. This deficiency leaves many organisations vulnerable, relying on outdated detection methods that AI-enhanced malware can consistently circumvent. Financial institutions are especially at risk, with average breach costs rising sharply, well above the global average.

As proactive measures, companies are starting to embrace hybrid defence strategies that blend AI with human expertise. This includes behavioural threat hunting, which utilises AI to establish baseline network behaviours and identify anomalies. Additionally, the adoption of adversarial training approaches—a technique that educates neural networks to withstand manipulation—has gained traction as a frontline defence method. Nevertheless, experts emphasise that combating the evolving AI threat landscape requires continuous education and upskilling for cybersecurity professionals to stay abreast of new challenges.

Regulatory bodies have begun to respond, implementing frameworks aimed at enhancing AI security. The EU's recent directive on watermarking synthetic content and the U.S. NIST's guidelines on model explainability are among the initiatives designed to bolster digital security in the age of AI. Yet, many security leaders argue that compliance efforts are lagging in response to the quickening pace of threat evolution, suggesting a pressing need for collaborative, real-time intelligence-sharing across sectors.

As these AI-driven threats proliferate, the distinction between state-sponsored cyberattacks and criminal enterprises is increasingly blurred. Forecasts predict more advanced AI-powered botnets capable of launching large-scale DDoS attacks, alongside the emergence of quantum computing that may enhance password-cracking capabilities. Such projections underscore the need for decisive action and comprehensive strategies in cybersecurity, as organisations risk catastrophic breaches if reliant solely on conventional, static defences.

In summary, while AI presents significant challenges to traditional cybersecurity paradigms, it also offers unprecedented opportunities for defence. By adopting hybrid frameworks that integrate human insight with technological advancements, businesses can better navigate the burgeoning complexities of a digital world increasingly shaped by AI.

### Reference Map

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

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

## Bibliography

1. <https://cybersecuritynews.com/artificial-intelligence-in-cyber-attacks/> - Please view link - unable to able to access data
2. <https://www.axios.com/local/indianapolis/2025/05/06/internet-crime-victims-cash-indiana-fbi> - In 2024, Indiana experienced a significant rise in internet crime, with residents filing 23,659 complaints—a 113% increase from the previous year—placing the state eighth in the nation for internet crime reports. Despite the record number of victims, financial losses dropped to $125.1 million from $162.2 million in 2023. Older residents, particularly those aged 60 and above, were the hardest hit, losing over $37.2 million. The FBI attributes the surge in cybercrime to advancements in artificial intelligence, which scammers use to create convincing text, images, audio, and video to execute fraud schemes more effectively. Tactics include social engineering, romance scams, and impersonation using voice and video AI tools. Nationally, internet crime losses soared to over $16 billion, marking a 33% increase. Authorities warn that actual losses may be higher, as fear and embarrassment prevent many victims from reporting. FBI officials emphasize that as technology advances, so do the tools and tactics used by cybercriminals, necessitating increased awareness and vigilance.
3. <https://www.techradar.com/pro/security/ai-is-making-phishing-emails-far-more-convincing-with-fewer-typos-and-better-formatting-heres-how-to-stay-safe> - A recent report by Cofense highlights the rising threat of AI-powered phishing campaigns, which have become increasingly sophisticated and harder to detect. Leveraging generative AI, attackers are producing more convincing emails with flawless grammar, authentic-looking sender information, and well-formatted content. These emails often impersonate company executives, integrate into existing email threads, and use lookalike domains to deceive recipients. In 2024, Cofense detected a malicious email every 42 seconds, with email scams up 70% year-over-year. Notably, many bypass traditional security tools due to polymorphic tactics that dynamically alter key message elements. Additionally, over 40% of malware samples in suspicious emails were newly seen variants, including Remote Access Trojans (RATs). To mitigate these threats, users are urged to scrutinize email content, verify internal requests independently, avoid relying on visual appearance, and utilize advanced security solutions that assess behavior beyond signature detection.
4. <https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/> - As AI technology becomes more widespread, the United Kingdom is expected to face an increase in both the frequency and severity of cyberattacks, according to Cabinet Office Minister Pat McFadden. Speaking at the CyberUK 2025 conference, McFadden announced the declassification of an intelligence assessment revealing that AI will escalate cyber threats in the coming years. In 2024, the National Cyber Security Centre (NCSC) received nearly 2,000 cyberattack reports, with 90 considered significant and 12 classified as highly severe—a threefold increase in major incidents from the previous year. Recent ransomware attacks have targeted notable British retailers including Marks & Spencer, the Co-op Group, and Harrods, resulting in significant operational disruptions. McFadden emphasized that cybersecurity is a vital necessity, not a luxury, and urged both public and private sectors to strengthen their defenses. The government plans to introduce a new cyber security strategy and legislate new powers under the upcoming Cyber Security and Resilience Bill. NCSC CEO Richard Horne also advocated for ending ransom payments to undermine the attackers' business model.
5. <https://www.axios.com/2025/05/06/ai-agents-identity-security-cyber-threats> - The cybersecurity sector is facing a new challenge with the rise of autonomous AI agents, prompting urgent efforts to manage them similarly to human employees. As companies increasingly adopt these agents for critical tasks, there's growing concern that without proper safeguards—such as credentialed identities and access controls—AI agents could inadvertently cause data breaches or leak sensitive information. This issue was a key focus at the recent RSA Conference in San Francisco. Deloitte predicts that 25% of companies using generative AI will launch autonomous AI pilots in 2025, with half adopting them by 2027. Although security professionals are experienced in managing nonhuman identities, AI agents pose elevated risks due to their potential autonomy within company networks. Awareness of these risks varies among organizations, prompting security vendors to educate executives about the urgent need for robust AI agent security. As agent deployment accelerates, establishing effective identity and access controls becomes crucial to maintaining trust, security, and compliance.
6. <https://www.reuters.com/sustainability/sustainable-finance-reporting/esg-watch-companies-complacent-about-cybercrime-despite-rise-risk-ai-2025-02-03/> - A recent meeting of the World Economic Forum (WEF) in Davos highlighted growing concerns over cybersecurity, given the complexity of the cyber landscape and increased risks due to technologies like artificial intelligence (AI). According to the WEF's Global Cybersecurity Outlook, geopolitical tensions are increasing cyberattacks by state and criminal actors. Sectors such as healthcare, financial services, and energy are particularly vulnerable. Caroline Escott of Railpen emphasized the importance of cyber resilience for investors, noting that many organizations have been affected by recent cyber incidents. Additionally, the lack of development in controlling technologies like AI is expanding the "attack surface" and facilitating more sophisticated attacks, such as deepfake scams. Cybersecurity regulation varies globally, with the European Union leading through recent directives requiring better resilience and security. The growing cybersecurity skills gap is also hindering effective management of cyber risks. Adopting a "zero trust" approach and requiring continuous proof of cyber defenses from providers are considered essential steps to improve security.
7. <https://www.axios.com/newsletters/axios-codebook-4c6813f0-a5ce-11ef-ad2a-91f707f80b70> - In today's newsletter, Arkose Labs' survey reveals that only 20% of companies feel very prepared to defend against AI-powered attacks, which have increased in frequency and sophistication due to generative AI. The survey highlights a disparity in confidence levels between executives and senior directors/managers regarding AI preparedness. Companies deploying AI security tools feel more confident, but AI also brings more sophisticated threats. CrowdStrike has identified a new China-linked cyber-espionage group, Liminal Panda, targeting telecom networks to spy on communications. This raises concerns about China's aggressive cyber tactics and potential geopolitical ramifications. Microsoft is unveiling new cybersecurity features at its Ignite event, including enhancements to Windows device recovery and changes in how security vendors access the Windows kernel. These updates aim to prevent global outages and improve system resilience. Other industry updates include legal actions by X against California and cybersecurity patches from Palo Alto Networks. Heather "Razzlekhan" Morgan receives an 18-month prison sentence for her role in the 2016 Bitfinex hack.