# The future of cybersecurity: AI as both a tool and a threat by 2025



The landscape of cybersecurity is poised for significant transformation as artificial intelligence (AI) increasingly becomes a tool for both cyber attackers and defenders by 2025. According to insights from Carl Froggett, Chief Information Officer at Deep Instinct, cyber attackers are leveraging AI capabilities more aggressively, significantly enhancing the sophistication and speed of their operations. As detailed in a report from Enterprise Security Tech, projected trends indicate that attackers will expand the use of AI from primarily conducting phishing attacks to orchestrating a complete range of sophisticated cyber moves throughout the entire kill chain.

The advancement of AI technology is set to play a critical role in weaponising zero-day vulnerabilities, streamlining the process of executing attacks. Such vulnerabilities pose a significant threat as they often exist within software systems but remain unaddressed by vendors, particularly in major sectors like healthcare and local government. These critical verticals struggle with outdated cybersecurity measures, leaving them susceptible to breaches even with well-configured systems.

The report highlights that supply chain vulnerabilities, especially those associated with cloud and Software as a Service (SaaS) platforms, will continue to serve as a focal point for exploitation by cybercriminals. The dramatic rise in data breaches, greater ransomware demands, and the increase in zero-day vulnerabilities in 2024 will likely be exacerbated in 2025. As organizations become prime targets, the exploitation of weak home office infrastructures presents an emerging concern, as many household devices and routers possess vulnerabilities that are not prioritised by vendors for timely patches.

On the defensive side of the equation, organizations are being compelled to redefine their cybersecurity strategies. A shift from traditional reactive detection methods to proactive prevention strategies is essential, according to Froggett. As threats evolve, so too must the defensive measures, particularly leveraging advanced AI technologies like deep learning (DL) to preemptively thwart attacks. DL distinguishes itself by its ability to process vast datasets and recognise subtle patterns, which aids in predicting and warding off previously unrealised threats.

Yariv Fishman, Chief Product Officer at Deep Instinct, emphasises that 2025 will see a critical escalation in demand for proactive defence strategies in reaction to sophisticated AI-driven threats harnessed from large language models, referred to as DarkAI. The traditional "assume breach" approach will diminish in favour of a prevention-first strategy encapsulated by Zero-Day Data Security (ZDDS). This approach proactively identifies and isolates potentially harmful files before allowing them access to secure network environments, thereby significantly bolstering an organisation's security framework against rapidly evolving cyber threats.

Furthermore, the cybersecurity sector is expected to invest heavily in real-time explainability technology that can help analysts discern legitimate zero-day attacks from false positives, a challenge that is exacerbated by the rapid pace of threat generation driven by generative AI. This technological progression underscores the increasing complexity and urgency needed in cyber defence strategies as organisations prepare for a future where the landscape is dominated by AI's capabilities on both sides of the cyber warfare divide.

As we move into the future, the interplay between advancing AI technologies, the sophistication of cyber threats, and the need for robust preventive measures positions 2025 as a pivotal year in the evolution of cybersecurity.

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

## Bibliography

1. <https://sosafe-awareness.com/company/press/one-in-five-people-click-on-ai-generated-phishing-emails-sosafe-data-reveals/> - Corroborates the use of AI in phishing attacks, highlighting that AI-generated phishing emails are highly successful and can be composed faster, increasing the danger due to their scalability.
2. <https://www.isaca.org/resources/news-and-trends/industry-news/2025/cybersecurity-trends-to-watch-in-2025> - Supports the trend of AI being used by both cyber attackers and defenders, and the need for advanced AI technologies in cybersecurity strategies.
3. <https://keepnetlabs.com/blog/top-30-phishing-statistics-and-trends-you-must-know-in-2024> - Provides statistics on the prevalence and impact of phishing attacks, which are expected to be exacerbated by AI technology in 2025.
4. <https://www.isaca.org/resources/news-and-trends/industry-news/2025/cybersecurity-trends-to-watch-in-2025> - Highlights the importance of AI governance and the role of standards like ISO/IEC 42001:2023 in managing AI systems, which is crucial for both attackers and defenders.
5. <https://keepnetlabs.com/blog/top-30-phishing-statistics-and-trends-you-must-know-in-2024> - Details the vulnerabilities in cloud and SaaS platforms, as well as the rise in data breaches and ransomware demands, which are expected to continue in 2025.
6. <https://sosafe-awareness.com/company/press/one-in-five-people-click-on-ai-generated-phishing-emails-sosafe-data-reveals/> - Emphasizes the difficulty in distinguishing AI-generated phishing emails from human-generated ones, underscoring the need for advanced detection methods.
7. <https://www.isaca.org/resources/news-and-trends/industry-news/2025/cybersecurity-trends-to-watch-in-2025> - Discusses the shift from reactive detection to proactive prevention strategies, including the use of deep learning to predict and ward off threats.
8. <https://keepnetlabs.com/blog/top-30-phishing-statistics-and-trends-you-must-know-in-2024> - Highlights the exploitation of weak home office infrastructures and the vulnerabilities in household devices and routers, which are not prioritized for timely patches.
9. <https://www.isaca.org/resources/news-and-trends/industry-news/2025/cybersecurity-trends-to-watch-in-2025> - Mentions the increasing complexity and urgency in cyber defence strategies due to the rapid pace of threat generation driven by generative AI.
10. <https://sosafe-awareness.com/company/press/one-in-five-people-click-on-ai-generated-phishing-emails-sosafe-data-reveals/> - Supports the idea that advanced AI models, such as Chat GPT-4, will make phishing attacks even more sophisticated and dangerous.
11. <https://www.enterprisesecuritytech.com/post/ai-s-double-edged-sword-navigating-cybersecurity-in-2025> - Please view link - unable to able to access data