NEWS

How can you protect your privacy, money from AI?

Expert explains the cybersecurity arms race focused on your data

March 25, 2025 | Author: Eric Baerren | Media Contact: Aaron Mills

Share

Artificial intelligence is playing an increasing role in cybersecurity, both as a threat and a defense. Central Michigan University computer science faculty Qi Liao answers questions about both.

Artificial intelligence is expected to touch every part of our lives. That includes a growing AI arms race in cybersecurity that places your privacy and financial data at risk in an increasingly sophisticated environment.

Qi Liao is a professor of computer science in Central Michigan University's Department of Computer Science. He shared his expertise on developments in cybersecurity related to artificial intelligence.

Q. How is artificial intelligence being used to launch cyberattacks?

Traditionally, artificial intelligence (AI) and machine learning (ML) have been powerful tools for cybersecurity defense, aiding in anomaly detection, intrusion prevention, spam filtering and mitigating threats like distributed denial-of-service (DDoS) attacks and malware.

However, in recent years, attackers have also begun leveraging AI and ML to launch sophisticated cyberattacks. For example, adversarial machine learning (AML) can be used to manipulate and poison training data, making defensive AI systems less effective. My research [1,2] has demonstrated that AML can generate spam emails capable of bypassing spam filters by tricking them into misclassifying harmful

Qi Liao

messages as benign.

In another study [3], we developed an AI system that autonomously exploited system vulnerabilities to gain administrative access. This was achieved by fine-tuning large language models (LLMs) with Retrieval-Augmented Generation (RAG), similar to the AI technology behind ChatGPT.

Beyond exploiting system weaknesses, AI is revolutionizing social engineering attacks. Attackers can now automate and personalize phishing schemes by analyzing social media data. AI-generated deepfakes, including realistic audio, video and images, have been weaponized for scams such as blackmail, impersonation and financial fraud. These tools enable attackers to execute crimes like online banking fraud, fake ransom demands and large-scale financial scams.

Q. What are the biggest privacy threats posed by AI-powered cyberattacks?

Data breaches remain the most significant privacy threat posed by AI-driven cyberattacks, and AI can enhance every stage of these breaches. Attackers use AI to generate and crack passwords, automate the exploitation of zero-day vulnerabilities, and deploy sophisticated phishing attacks to deliver malware such as ransomware and computer virus.

Our research findings [4,5,6] suggest that "ransomware 2.0", which not only locks victims out of their data but also steals and sells it, will become the dominant form of attack. This evolution increases the damage inflicted, as attackers can both demand ransom and profit from selling stolen data.

Even publicly available data can compromise user privacy when processed with AI. Photos, videos and audio recordings shared on social media can be manipulated to create deepfake content for identity fraud. AI algorithms can also cross-reference and correlate anonymized data from medical, financial and voter records, as well as smart home and mobile device activity, effectively re-identifying individuals and revealing their behavior patterns.

Q. How can AI cyberattacks impact my financial security?

AI-powered attacks pose a serious risk to financial security by enabling fraud, identity theft, and large-scale scams. For example:

- AI-generated deepfake videos can impersonate an employer, instructing an accountant to transfer funds.
- Attackers can create fake hostage videos, where a cloned voice or face of a loved one demands ransom.

AI can generate fake blackmail schemes, using fabricated images or videos to extort money.

Beyond impersonation, AI-driven attacks can compromise bank security questions by analyzing publicly available personal data, enabling identity theft and fraudulent account creation. AI can also automate ransomware attacks that steal financial information, such as credit cards and bank details and high-value cryptocurrency wallets.

One emerging scam, the “pig butchering” scheme, uses AI-powered chatbots to build long-term trust with victims in online relationships before convincing them to invest in fraudulent, high-return financial schemes.

Q. Are AI-driven cyberattacks more difficult to detect and defend against?

Yes, AI-powered attacks are increasingly difficult to identify and counter. A good example is the challenge educators face when students use generative AI to complete assignments. While AI detection tools exist, they are not foolproof, and some students have even used AI to evade AI by manipulating AI detection scores.

Similarly, deepfake detection technologies exist, but they struggle to keep pace with AI advancements. The cybersecurity landscape is caught in a constant arms race, where attackers and defenders continuously improve their tactics, much like the ongoing battle between evolving viruses and vaccines.

AI also lowers the barrier to entry for cybercriminals. Previously, launching a cyberattack required expertise. Now, AI enables even non-experts to execute highly effective attacks. My current research explores what happens when both attackers and defenders use AI, studying adversarial mutual machine learning within a game-theoretic framework to understand this dynamic.

Q. What can individuals do right now to protect themselves from AI-enhanced cyber threats?

Adopting a zero-trust mindset is key. Always remain vigilant against AI-powered phishing and scams. Here are some essential steps:

- Be skeptical of all digital interactions. What appears to be a real person, whether on a video call or in a message, may be AI-generated. Consider establishing a secret word with close family and friends for verification.
- Limit social media sharing. Publicly shared personal information can be weaponized by AI against you.
- Be cautious with unknown calls. AI-powered robocalls can clone your voice. When answering calls from unknown numbers, let the other party speak first.
- Use strong, unique passwords and enable multi-factor authentication for all accounts.
- Back up and encrypt important data regularly to prevent loss from ransomware attacks.
- Stay informed. Keep up with cybersecurity developments and consider formal training. At Central Michigan University, we offer cybersecurity degrees and certification programs covering cryptography, network security, software security, hardware security, social engineering and AI/ML in cybersecurity.
- Finally, we cybersecurity researchers must develop next-generation defense mechanisms to stay ahead of the new AI-driven cyberattacks. The battle against AI-powered threats is ongoing, and proactive adaptation is our best defense.

About Qi Liao

Qi Liao is a professor of computer science in Central Michigan University's Department of Computer Science. He received his bachelor's degree in computer science from Hartwick College, and his master's and doctorate degrees from the University of Notre Dame.

His research interests include artificial intelligence and machine learning, computer and network security, economics and game theory of networks and cybersecurity, and visual analytics. More information may be found at https://people.se.cmich.edu/liao1q/.

References:

[1] Bhargav Kuchipudi, Ravi Teja Nannapaneni, and Qi Liao. Adversarial machine learning for spam filters. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES) - 15th ACM International Workshop on Frontiers in Availability, Reliability and Security (FARES), number 38, pages 1-6, Dublin, Ireland, August 25-28 2020.

[2] Jonathan Gregory and Qi Liao. Adversarial spam generation using adaptive gradient-based word embedding perturbations. In IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things, (AIBThings), pages 1–5, Central Michigan University, USA, September 16-17 2023.

[3] Jonathan Gregory and Qi Liao. Autonomous cyberattack with security-augmented generative artificial intelligence. In IEEE International Conference on Cyber Security and Resilience (CSR), pages 270-275, London, UK, September 2-4 2024.

[4] Zhen Li and Qi Liao. Preventive portfolio against data-selling ransomware - a game theory of encryption and deception. Computers & Security, 116:1–11, Article 102644, May 2022.

[5] Zhen Li and Qi Liao. Game theory of data-selling ransomware. Journal of Cyber Security and Mobility, 10(1):65-96, March 2021. DOI: 10.13052/jcsm2245-1439.1013.

[6] Zhen Li and Qi Liao. Ransomware 2.0: To sell, or not to sell a game-theoretical model of data-selling ransomware. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES) - 9th ACM International Workshop on Cyber Crime (IWCC), number 59, pages 1-9, Dublin, Ireland, August 25-28 2020.

VIEW LATEST NEWS

Share

f 𝕏 in

Related News