

Get Ready for a Catastrophic Leak That Reveals All Your Messages and Search History

"Companies are getting hacked every single day."

By [Maggie Harrison Dupré](#)

AI is revolutionizing cyberattacks, as advancements in the tech allow bad actors to find and exploit unknown vulnerabilities in software across the web. If there were ever a time to shore up your security habits — or maybe just nuke your entire digital history — it's now.

A pair of terrifying stories dropped this week highlighting exactly how vulnerable all of us are right now. One, [published in *New York Magazine*](#), was a chill-inducing reminder of exactly how revealing the past 20 years of simply existing on a web run by data-storing tech giants — social media, email, iMessage, online health and banking, pornography, buying anything and everything — really is. And an [article published in *The Atlantic*](#) stressed how vulnerable institutions ranging from corporate giants to banks to utilities and government agencies currently are to AI-powered cyberattacks.

In short, recent AI coding advancements have effectively dropped bad actors in a vat of radiation and transformed them into AI-fueled supervillains — and companies, which are often tasked with protecting important information about consumers, are racing to keep up with the onslaught of attacks.

"There's a crazy amount of offensive activity happening right now," Alex Stamos, a former chief security officer at Yahoo and Facebook, told the *Atlantic*. "Companies are getting hacked every single day."

Per the *Atlantic*, the security company Palo Alto Networks has reported a staggering year-over-year increase in daily attacks, with hackers developing unsettling tactics like self-modifying viruses. The magazine also pointed to data from the credit giant Moody's Ratings, which has found that, as of 2025, it takes bad actors roughly 44 days or so to exploit a known security vulnerability — a striking figure when contrasted to a 700 day average as of 2020. Institutions are rushing to issue patches over security gaps, but it's basically impossible for them to outpace the speed at which bad actors are deploying AI against them.

If there's any bright spot, advanced AI models like Anthropic's much-hyped Mythos model have [helped](#) companies sweep their existing code for vulnerabilities in a push to get ahead of attackers. Even so, right now, digital weapons are looking more promising than digital armor.

More on AI and cybersecurity: [Microsoft's Copilot AI Caught Letting Hackers Steal Your 2FA Codes Through a Single Click](#)