

Will hackers use more AI in ransomware attacks in 2025?

Short answer: Yes. Attackers are expected to keep expanding their use of artificial intelligence, especially large language models, to impersonate trusted individuals and manipulate victims into granting access or trust.

Why AI Has Become a Hacker Favorite

Search results, news feeds, and everyday conversations are now saturated with AI references, and that same enthusiasm has taken hold among cybercriminals. When most people mention AI, they are typically referring to large language models like the ones behind ChatGPT and similar tools that can convincingly mimic human communication. Attackers have recognized that this capability is extremely useful for social engineering. Rather than relying on generic phishing emails, they can generate messages, voices, or conversations that closely resemble a real colleague, vendor, or authority figure, making it far easier to earn a target's trust before striking.

Expect More Refined Impersonation Tactics

The trend heading into 2025 is not that AI-driven attacks are brand new, but that they are becoming more polished and business-like. In the same way legitimate companies are rolling out AI-powered sales agents and automated outreach tools, attackers are refining their own AI-driven impersonation techniques. This means more convincing messages that mimic bosses, coworkers, or trusted partners, all designed to exploit the working relationships people rely on every day. The danger is that a conversation which feels personal and legitimate may actually be coming from a highly capable AI system built to manipulate, not assist.

What This Means for Defense

As these impersonation tactics mature, organizations should assume that trust-based attacks will become harder to spot through instinct alone. Verifying requests through independent channels, rather than trusting a message or call at face value, becomes increasingly important. Because these attacks are designed to bypass human judgment, having automated detection and response capabilities in place, such as those built into Cyber Crucible's FortressAI, provides an additional

layer of protection when social engineering succeeds in getting past a person's defenses.

<https://player.vimeo.com/video/1046827321>

[Watch on Vimeo](#) · Captions: English, Français, Español, العربية

Revision #4

Created 2026-07-23 23:18:00 UTC by Dennis Underwood

Updated 2026-07-24 00:31:23 UTC by Dennis Underwood