Hogan Lovells

News

Confronting social engineering in the age of artificial intelligence

19 February 2025

AI-enabled technology enhances threat actors' ability to engage in advanced and difficult-to-detect forms of social engineering to deceive employees and circumvent companies' security controls. Companies may consider new measures to address these emerging vulnerabilities.

At the core of cybersecurity are human relationships, interactions, and decisions. When discussing cybersecurity, the imagination often conjures images of reclusive, hooded hackers, typing away at a nondescript page of code to manually bypass complex, technical security controls. While threat actors no doubt make use of sophisticated tactics and exploit technical weak spots in target companies' environments, most cyberattacks hinge on the deception of other human beings. Commonly referred to as social engineering, threat actors use trickery and psychological manipulation to bypass companies' security safeguards. Social engineering exploits common desires, instincts, and social dynamics – a special one-time discount offer, an urgent email from a familiar-looking email address, or an unassuming message from tech support can all be fronts for a legitimate security threat, each designed to prompt a response from the recipient that helps a threat actor further their objective.

The dangers of social engineering are well-established and ubiquitous. One source estimates that 98% of cyber attacks involve some degree of social engineering, while another source estimates that an average organization is targeted by over 700 social engineering attacks every year. Employees are often given trainings on the dangers of phishing and other social engineering tactics, and companies are well-aware that security incidents frequently manifest due to some kind of human error. However, as the use of artificial intelligence (AI) proliferates, so too do the risks of AI-enabled social engineering threats. AI is increasingly being leveraged by threat actors to augment their social engineering campaigns, enabling methods that are hard to detect due to their realism, deeper insights about targets, and heightened capacity to communicate in foreign languages.

AI makes social engineering easier and harder to detect

Social engineering can be broken down into four general steps. First, the threat actor must research the target. A threat actor investigates its target's background and pulls information about them so it can best tailor its communications to them. Second, the threat actor contacts the target(s), and provokes a response from the target by establishing trust, manufacturing a feeling of urgency, or by promising some sort of incentive or reward. Third, the threat actor coaxes the desired information from the target(s). Fourth, the attacker performs their "get away," obscuring traces of their activity. While performing high-quality social engineering campaigns was once a costly and time-intensive exercise given the effort needed to research individuals and prepare convincing communications to deceive them, AI makes it substantially easier to mine data about an individual and to construct convincing campaigns. Malicious AI tools can be used to build a profile of a target based, for example, on that individual's social media and online presence. Autonomous agents and other AI-powered tools allow large-scale targeted phishing operations.

AI also makes it much easier to build trust and to bypass individuals' suspicions. Generative AI already allows foreign threat actors to communicate with targets more effectively in the target's language, be it through AI tools that can remove grammatical and spelling mistakes or translation technology that can tailor communications to regional dialects. In the coming year, there may also be an increased use of advanced video deepfakes and voice cloning technology to drive sophisticated social engineering campaigns. For example, consider a scenario in which a threat actor sends an email to an employee, masquerading as the employee's boss. A single call or video teleconference could verify

whether the request was coming from the actual boss. Now, AI-enabled deepfakes and voice cloning allows threat actors to convincingly communicate with targets live while impersonating another person, even on a video teleconference.

Compounding these risks is the fact that many AI tools that enable social engineering are based on free, open source intelligence like web reconnaissance software Recon-ng, and are trained on vast quantities of publicly-available data that can provide detailed accounts of individuals' lives.

Combatting AI-enabled social engineering

Though the threats are significant, and increasingly difficult to detect, there are many actions companies may consider to mitigate AI-enabled social engineering.

- **AI-based controls.** AI-powered tools can also be used to detect, identify, and respond to more sophisticated social engineering tactics.
- **Bolstering authentication.** Companies can evaluate ways to enhance their authentication process, taking into account voice cloning and deepfake technology that can potentially bypass audio/video-based authentication systems.
- **Training and awareness.** Companies may consider hosting trainings to educate employees on social engineering that leverages AI, teaching individuals how to proceed cautiously in the face of increasingly convincing threat actor communications.
- **Updating policies and procedures.** Consider whether current policies and procedures have a system in place to review and respond to reports of advanced social engineering, and whether new procedures must be implemented to account for increasingly sophisticated tactics.
- **Harden accounts payable processes.** A common goal of many social engineering attacks is to trick a company into sending funds to a malicious account. To help mitigate these risks, companies may consider developing more robust verification processes for accounts payable teams, allowing these teams to distinguish legitimate requests to, for example, update a bank account number, from malicious ones. For example, companies that require the CFO to sign off on wires over a certain amount may consider establishing a secret password that the CEO will say over the phone when authorizing one.

Next Steps

While artificial intelligence allows threat actors to greatly enhance their social engineering tactics, companies still have many tools and resources at the disposal to combat them. As technologies continue to evolve, companies may wish to stay apprised of the emerging risks while taking proactive steps to confront them.

Contacts

Nathan Salminen

Partner

Washington, D.C.

Email me

Ryan M. Campbell

Associate

Washington, D.C.

Email me