Lookout™

Mobile Threat of the Month

March 2025

Social Engineering in the Era of Generative AI: A Growing Threat to Cyber Security

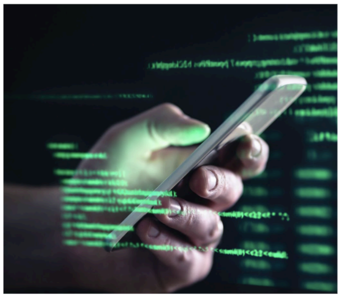
How Attackers Leverage AI

In the ever-evolving landscape of cybersecurity, social engineering has long been a potent tool for attackers. By exploiting human psychology rather than technical vulnerabilities, cybercriminals manipulate individuals into divulging sensitive information or granting unauthorized access. Generative AI has elevated this threat to unprecedented levels, making social engineering attacks more sophisticated, personalized, and difficult to detect.

AI-generated emails can now mimic the writing style of a colleague or executive with alarming accuracy. Similarly, deepfake technology can produce fake video or audio messages that appear to come from trusted sources. The scale and speed at which generative AI operates amplifies the problem.

Common social engineering mobile attacks include:

- Phishing, smishing (SMS-based phishing),
- Pretexting (posing as a trusted entity, e.g., exec impersonation),
- Baiting (luring victims into downloading malware),
- Vishing (AI-generated voice/video call scams).



Potential Impact

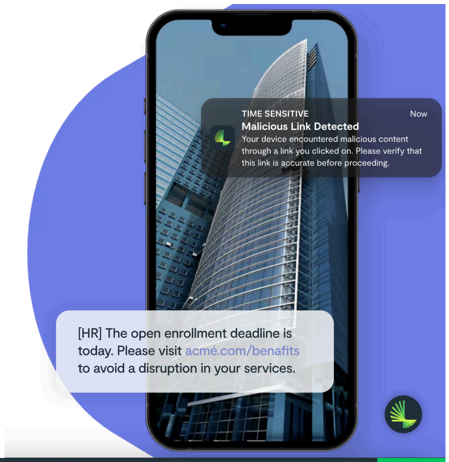
The consequences of advanced social engineering attacks are severe. Organizations risk financial losses, reputational damage, and regulatory penalties, while individuals face identity theft, financial fraud, and emotional distress. The rise of generative AI has outpaced traditional security measures like email filters and antivirus software, making it increasingly difficult to defend against these evolving threats.

A single vishing attack last year demonstrates the growing sophistication and potential impact of AI-based cyber-attacks. A deepfake video used generative AI to create an avatar that convincingly impersonated a company's Chief Financial Officer during a live conference call. An employee at the multinational firm was scammed into paying out $25 million to fraudsters.

Lookout Mobile Security

Cyber security awareness training to educate employees to spot the signs of cyber attacks has become less effective as AI based social engineering attacks become increasingly unrecognisable. To combat these risks, organizations should adopt a cybersecurity approach that includes advanced AI-powered threat detection to identify and mitigate social engineering attempts.

Lookout's social engineering protection technology is built to detect AI-created cyber-attacks that target mobile devices by leveraging its own large dataset and language models (LLMs). These LLMs are trained to analyze SMS messages and websites for indicators of potential attacks or phishing such as urgency, impersonation, and requests for sensitive information. Like all AI systems, Lookout's cloud-driven dataset continually evolves, learning from emerging threats to improve detection accuracy and adapt to developing attack strategies.



TIME SENSITIVE Now
Malicious Link Detected
Your device encountered malicious content through a link you clicked on. Please verify that this link is accurate before proceeding.

[HR] The open enrollment deadline is today. Please visit acmé.com/benafits to avoid a disruption in your services.