How AI is Supercharging the Next Wave of Phishing Scams

Artificial intelligence (AI) has transformed industries in incredible ways, but it's also become a powerful tool for cyber criminals, especially in making more realistic phishing scams. Phishing, where attackers trick people into handing over sensitive information, has become more dangerous and sophisticated, thanks to AI. From crafting believable fake emails to automating mass attacks, AI is reshaping the landscape of phishing.

**The Growing Threat of AI-Powered Phishing**

Phishing attacks are on the rise. In fact, according to [Zscaler’s 2024 Phishing Report](https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report), they surged by 58% in 2023 alone, with AI playing a major part in this increase. AI enables attackers to create highly personalised phishing messages by scanning social media and other online sources for data. These customised messages are harder to spot because they look more authentic, matching the recipient's personal or professional details.

Cyber criminals are using AI to mimic the writing style of trusted contacts, making phishing emails almost identical to legitimate ones. This added layer of deception makes it incredibly hard for individuals to identify when they're being targeted.

**How AI is Crafting Convincing Phishing Emails**

AI’s ability to generate natural-sounding language has drastically improved the quality of phishing emails. Tools like natural language processing models allow attackers to create messages that are grammatically flawless and contextually accurate. Gone are the days of obvious spelling mistakes and weird phrasing. Phishing emails can look and sound just like genuine ones.

For example, AI-powered tools can perfectly copy the communication style of an executive, making it easy for employees to fall for business email compromise (BEC) scams. Cyber criminals can even analyse the online behaviour of individuals or companies and use that data to send highly specific phishing emails. These personalised messages often feel more trustworthy, making people more likely to click on malicious links or download harmful attachments.

**Automating Phishing Campaigns with AI**

AI isn’t just making phishing emails more convincing, it’s also helping cybercriminals scale up their attacks. With AI-powered automation tools, attackers can launch massive phishing campaigns in minutes. Thousands of emails, each customised for the recipient, can be sent out effortlessly. Unlike traditional phishing attempts, where everyone receives the same generic email, AI-driven attacks feel personal, making them far more effective.

Research by [Microsoft](https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/how-ai-changing-phishing-scams) highlights how AI can generate thousands of personalised phishing emails in seconds. Instead of just targeting people with basic information, cyber criminals can use AI to gather data from social media, public records, and company websites, crafting highly targeted phishing attempts that are much harder to detect.

**Defending Against AI-Powered Phishing Attacks**

As AI continues to enhance phishing attacks, defending against them requires an equally sophisticated approach. Organizations and individuals need to be aware of the increased threat and take steps to protect themselves:

* **Be Sceptical of Unusual Emails or Messages**Even if an email looks legitimate, think twice before clicking on links or downloading attachments. Check for small details like odd email addresses or unexpected requests.
* **Verify Before You Act**If you receive an urgent email asking for sensitive information, money transfers, or password resets, verify it by contacting the person directly using known contact methods (not the info in the email).
* **Use Multi-Factor Authentication (MFA)**  
  Always enable MFA for important accounts. It adds an extra layer of security by requiring a second form of verification, like a code sent to your phone.
* **Keep Your Software and Security Tools Updated**Regularly update your devices and security software to protect against the latest phishing threats. Hackers exploit outdated systems.
* **Learn to Spot Phishing Red Flags**Watch out for unusual links, spelling mistakes, suspicious attachments, or messages that pressure you to act quickly. Trust your instincts—if something feels off, it probably is.
* **Be careful what you share on Social Media**  
  Cybercriminals can use your social media info to personalise phishing attacks. Be mindful of what you post and keep your privacy settings tight.
* **Report Suspicious Emails or Messages**If you come across a phishing attempt, report it to your organisation’s IT or Cyber team. Reporting helps prevent others from falling victim to the same attack.