SECURITY INSIGHTS:

Phishing is Getting Trickier: What You Need to Know

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

Even with years of training, phishing is still a major problem. But cybercriminals are getting much smarter, making phishing attacks harder to spot and more dangerous. They are changing their methods to look more real, bypassing security checks, and targeting people more specifically.

Here's how cybercriminals are making phishing more potent than ever:

They're Getting Clever with Generative AI

Criminals are using Artificial Intelligence (AI), especially generative AI, to make phishing emails look more convincing. This AI can copy writing styles and create emails with perfect spelling and grammar, avoiding the usual red flags. It can also personalize emails using information found online. Tools like WormGPT and GhostGPT, which use powerful AI, are helping create these realistic emails, even generating fake login pages. This means phishing emails can now sound much more authentic and less suspicious.

They're Luring with Voice and Video

AI is also being used to clone voices and appearances from online audio or video. Combined with tools that can fake caller ID, criminals can call targets pretending to be someone they trust, like a family member, friend, or coworker, and ask for urgent help. These calls can sound very convincing, mimicking the person's voice and how they talk. This technology is already being used, and we can expect to see more sophisticated attacks using AI for voice and video in the future.

They're Resurrecting Fake 'Threads' and Reply Chains

Criminals are taking old email conversations that were hijacked and adding new, fake emails to the chain. These "zombie" threads are becoming more believable with the help of generative AI. AI can analyze the previous emails in the chain and create a new phishing email using the right tone and context, making it seem like a legitimate reply from the original sender.

They're Running ClickFix Attacks to Dupe the PowerShell Naive

A newer technique called ClickFix involves sending emails with links that, when clicked, ask the victim to copy and paste a command into a box on their computer. This is often presented as a way to "fix" a problem mentioned in the email. These attacks use common tricks, like emails about fake invoices or documents, to convince users to run a harmful command that installs malware.

They're Impersonating Trusted Brands More Convincingly

Criminals continue to pretend to be well-known companies to trick people into giving up information or clicking on malicious links. They often impersonate platforms people use daily, like Microsoft's OneDrive, SharePoint, and DocuSign. By copying the look of login pages for these services, attackers can steal usernames, passwords, and even multi-factor authentication details. They use convincing techniques like fake sender addresses and slightly altered website addresses that look real.

They're Abusing Trusted Services

Another trick is to use legitimate document-signing or file-hosting websites to store and distribute phishing content. Attackers upload malicious files to services like Google Drive or Dropbox and then send phishing emails with links pointing to these services. Because the links look like they go to a trusted site, users might not be suspicious, and these attacks can bypass some security systems.

They're abusing QR Codes

QR codes are now being used in phishing attacks, a technique sometimes called "quishing". Since many email filters flag suspicious links, criminals are embedding malicious QR codes in emails instead. These codes can be disguised as requests for multi-factor authentication, delivery notifications, or login prompts. Scanning the code leads to a fake website designed to steal credentials. Some sophisticated attacks even use multi-stage quishing, where the QR code first leads to a seemingly safe page before redirecting the user to a fake login site, especially targeting mobile devices, which may have less security.

They're Leaning on Images to Bypass Security Filters

Image-based phishing is also evolving. Criminals are creating images that look exactly like text-based emails, which helps them bypass traditional security filters that scan for text. These images often contain links or hidden malicious content. Attackers might even change the images slightly over time to avoid detection.

They're Supercharging Intel Gathering

Criminals are using AI-powered tools, often found on the dark web, to gather information. These tools can automatically collect details from social media posts, sometimes even figuring out a user's location. Other tools focus on gathering information about companies, scraping data from sites like LinkedIn, recruitment sites, and public records to identify potential targets and learn about their technology or employees. They can even use legitimate marketing tools to find the best ways to reach victims.

They're Professionalizing with PhaaS

Phishing has become a service that criminals can buy. Phishing-as-a-service (PhaaS) platforms offer tools and services like dashboards and ways to store stolen information, making it easier for even less skilled criminals to launch attacks. They are getting more advanced, with some platforms able to steal multi-factor authentication codes.

Phishing is constantly evolving, with cybercriminals using new technologies and tactics to increase their success. Being aware of these methods is crucial for staying safe online.