Phishing in 2024: What the Lures Look Like and How Not to Get Caught

In the old days (that is, a couple of years ago), grammar mistakes and clumsy attempts to personalize signaled a possible phishing attack. Unwary users still got caught, but common sense and email filters provided pretty good protection. Phishing in 2024 has evolved to a more dangerous level, and both users and organizations need to strengthen their defenses.

Recent studies show an alarming increase in phishing attacks. A study by Acronis, for instance, reports an increase of over 200% in email attacks just in the last six months. Despite being one of the oldest attack vectors, email remains one of the most effective. And with generative AI reaching mainstream, threat actors have taken their attacks to new levels of sophistication.

AI Has Changed the Face of Phishing in 2024

AI has transformed the way we research and create. It has changed the way we analyze and protect data. And it has also revolutionized the way cyber criminals wage war. Gone are the days when hackers had to manually comb through social media to craft a phishing email personalized enough to succeed.

Now threat actors use large language models (LLMs) to harvest detailed data about people and organizations in mere seconds. These details make phishing emails much more believable and help hackers create a sense of urgency. Generative AI increases the authenticity by making it easy to eliminate spelling and grammar errors and mimic writing styles.

Imagine receiving an email from a work friend that references a party you both attended last night. The friend knows your nickname, details of a recent project you blogged about. And she needs your password to access a key file. You trust her, you work closely together, and the email sounds like one she would send. You give her the password and…disaster.

AI also helps attackers automate phishing campaigns and bypass traditional security measures. Enterprising cyber criminals have created sophisticated phishing kits, making them available for an attractively low cost. Hackers thus gain access to phishing templates, anti-detection tools, and even technical support.

Multi-channel Attacks Exploit Gaps in Defenses

Threat actors increasingly use multiple attack methods in addition to email, including texts, social media messaging, and voice calls. For instance, the victim might receive an initial email with a follow-up phone call or text to add legitimacy. Due to lax security on most mobile devices, mobile messaging proves scarily effective.

The rise of generative AI has also increased the sophistication of deepfakes. Attackers can clone voices and create highly realistic fake videos. When you hear your boss's distinctive gravelly voice on the phone, for instance, you will take the call seriously.

Layered Defense Critical…But Needs Updating

With deepfakes so convincing and AI attacks capable of bypassing email filters and even MFA, how do organizations protect themselves? The answer lies in a combination of advanced security tools and improved training.

To begin with, AI can help address the problem it created. Ironically, AI-powered email security prove rather efficient at detecting AI-generated content. And security tools that use machine learning and behavioral analysis identify phishing by analyzing multiple signals. These signals can include a structural analysis, body copy, images, links, and attachments.

Organizations should also update their authentication methods and privilege management. For instance, implementing passwordless authentication and a zero-trust approach provide additional protection. And security teams should regularly review privileged accounts, ensuring that user accounts have only the access they need.

Because 2023 also showed an upward trend in supply chain attacks, businesses should take a particularly close look at vendor access. A successful phishing attack on a vendor could result in the compromise of a trusted third-party account. Thus, in addition to implementing zero trust, businesses should regularly assess the security postures of vendors in the supply chain.

Finally, organizations must educate their employees, but they need to do it effectively. Security awareness training should be personalized to the team and, ideally, the individual. Again, AI can help with this. Phishing simulations also prove much more effective than traditional training alone.

Take the Next Steps to Protecting Critical Data

Sophisticated threats require a sophisticated approach to cyber security. Companies should start with a risk assessment to highlight vulnerabilities. And they should carefully evaluate their security controls, email filters, and security awareness training, updating as necessary. The email experts at Messaging Architects can help.