Courtesy of
MST Insurance Solutions, Inc.

Artificial Intelligence and the Increasing Threat of Phishing to Businesses

Phishing attacks, in which cybercriminals manipulate users into disclosing sensitive information or installing malware through fraudulent communications, have been a persistent cybersecurity threat, often resulting in significant financial and reputational damage. Recently, cybercriminals have begun leveraging artificial intelligence (AI) to power these attacks, making them more convincing and difficult to detect.

As this evolving risk continues to emerge, businesses must stay informed about the latest developments and implement adequate safeguards to mitigate its impact. This article provides an overview of the evolution of phishing in the age of AI, describing how this technology is transforming phishing attacks. It also examines the impact of these scams and offers steps businesses can take to safeguard themselves.

The Evolution of Phishing in the Age of AI
Traditional phishing attacks are more generic, prone to errors and contain red flags (e.g., misspellings, incorrect names and grammatical errors) that are relatively easy to spot. AI-powered phishing attacks, on the other hand, are highly personalized, linguistically polished and difficult to differentiate from legitimate communications.

These types of cyberattacks are also more easily scalable and increasingly targeted. For example, AI-led attacks may use “spear-phishing” schemes, in which fraudulent communications are sent to specific recipients, or business email compromise (BEC) tactics, where cybercriminals impersonate business leaders (e.g., CEO or partner) by hacking into their account or creating a realistic counterfeit message with an illegitimate request for sensitive information or payment.

How AI Is Transforming Phishing Tactics
AI is changing traditional phishing tactics in several key areas, including:

- **Personalization and social engineering**—AI can analyze vast datasets, including social media posts, websites and public records, to craft highly tailored messages. It can be trained to mimic writing styles to appear authentic, reference specific details (e.g., recent purchases, ongoing projects) to seem legitimate, and even clone the voice of business leaders or generate realistic videos to make fraudulent yet convincing messages.
- **Automation and scale**—AI enables the mass generation of unique phishing messages in a matter of minutes. This allows cybercriminals to increase their output of illegitimate communications, thereby raising their chances of successfully tricking a user into providing sensitive information or installing malicious software.
- **The bypassing of traditional defenses**—Due to its increasing sophistication, AI-crafted communications can evade rule-based filters and signature-based detection. This means that organizations relying on traditional safeguards against phishing attacks may be vulnerable to AI-powered scams.

The Impact of AI-driven Phishing on Businesses
AI-powered phishing attacks have numerous impacts on businesses. Because AI can increase cybercriminals’ output volume and enhance the sophistication of their tactics, employees may encounter multiple fraudulent messages on a daily basis. The combination of frequent attempts and convincingly crafted messages may

MST INSURANCE SOLUTIONS

increase the likelihood that a business will fall victim to one of these scams.

Once infiltrated, an organization may suffer significant financial losses through BEC, fraudulent wire transfers, illegitimate payments or data breaches. It may also face substantial business interruption as the attack is investigated and remediated. Additionally, AI-driven phishing attacks create challenges for IT teams, who must address the expanding attack surface, monitor the use of unapproved hardware or software ("shadow IT") and manage cyber risks stemming from a remote or hybrid workforce.

Steps Businesses Can Take to Protect Themselves
Although AI-powered phishing attacks present new threats and challenges, employers can take several steps to protect themselves:

- **Deploy advanced security solutions**. Utilizing anti-phishing software with AI-driven detection capabilities and context-based defenses can help a business's security systems evolve as the attacks evolve. AI-powered security can help detect unusual language use, patterns and requests, filtering suspicious emails. Encryption keys and login credentials should be rotated regularly to prevent exploitation.
- **Strengthen email and identity security**. Employers should implement multiple measures to ensure email accounts are secure. Requiring multifactor authentication and routinely changing strong, unique passwords can make it more difficult for cybercriminals to infiltrate them. Email filters, firewalls, email authentication protocols and other security measures should also be utilized. Employees should continue to check for signs of traditional phishing attacks (e.g., typos) and carefully verify links and attachments before opening them.
- **Educate and empower employees**. Staff should receive ongoing security awareness training that teaches them about the latest cybersecurity threats and hackers' newest tactics. Businesses should conduct phishing simulations to help employees recognize and respond effectively to fraudulent communications. Employees should feel empowered to verify requests for sensitive information before responding to them, especially those involving financial transactions or credential sharing, and they should be encouraged to report suspicious activities.
- **Develop comprehensive policies and incident response plans**. Clear data protection policies should be created, communicated and enforced. They should also be regularly reviewed and updated to respond to emerging cyberthreats. Additionally, incident response plans should be in place to mitigate the impact of phishing attacks, BEC scams and other cybersecurity incidents.
- **Leverage human and AI collaboration**. Combining AI and machine learning tools with human oversight can strengthen a business's cybersecurity posture. This collaboration can create holistic, adaptive defenses. Leveraging the strengths of human judgment and AI that is continually trained on phishing detection can enable a business to establish a defense system to prevent cyberattacks and respond rapidly to cybersecurity incidents.

Conclusion
AI-powered attacks are a growing threat to all businesses, regardless of their size or industry. By being aware of these scams and implementing cybersecurity measures to address them, organizations can enhance their cyber defenses and mitigate associated risks.

Contact us today for more information.