Unchartered Waters: The AI Phishing Wave Is Here

Articles

11.27.2024

Attorneys, Kate A. Sherlock and Nicholas T. Franchetti, authored the article, "Unchartered Waters: The AI Phishing Wave Is Here," for the *New Jersey Law Journal* writing, "AI is poised to make both traditional and spear phishing cheaper and more effective." For traditional phishing, AI can generate and send thousands of emails in virtually no time, whereas an individual threat actor would have needed minutes or hours to write each underlying email. Moreover, as AI has become more sophisticated, studies have shown that AI-generated emails are now indistinguishable from those written by humans. AI's effect on spear phishing has been even more pronounced.

These AI-generated phishing attempts not only pose direct financial danger to companies but they can also subject companies to civil or criminal liability under state and federal privacy laws. Many companies store sensitive protected information, such as customer health or financial information, which requires the company to implement commercially reasonable measures to protect that information.

While the cybersecurity landscape is constantly evolving, there are some best practices that companies should implement to minimize the risks associated with AI-enhanced phishing. First, companies should implement layered technological security measures, such as email filtering, authentication protocols, disabling links to dangerous websites, antivirus and antimalware, firewalls, and other tools to attempt to detect or at least flag suspicious emails. Companies should also highlight emails that originate externally to avoid the possibility of scammers masquerading as a co-worker. Additionally, companies should conduct comprehensive cybersecurity evaluations of new vendors, before engaging them, in order to understand the vendor's cybersecurity standards and data breach notification procedures.

The final line of defense for any phishing scam is the user. As such, companies should adopt comprehensive policies that cover password security, verifying information for financial transactions, and other cybersecurity vulnerabilities. Most importantly, companies need to regularly train their employees on the dangers of phishing scams and how to detect them, such as incorrect email addresses and emails that create an unexpected sense of urgency. Given the increased sophistication of phishing schemes due to the rise in AI, employees should be encouraged to carefully scrutinize sender email addresses and links, downloads, and requests for information from all sources.

To read the complete article, click here.

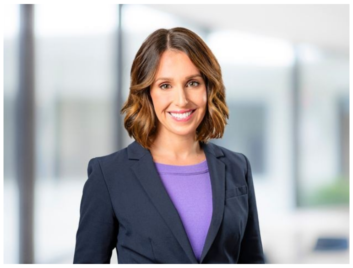
Related People

Nicholas T. Franchetti

Associate

✉ nfranchetti@archerlaw.com

☎ 856.857.2786



Kate A. Sherlock

Partner

✉ ksherlock@archerlaw.com

☎ 856.673.3919