ALM | LAW.COM

New Jersey Law Journal

Unchartered Waters: The AI Phishing Wave Is Here

By Kate A. Sherlock and Nicholas T. Franchetti

November 27, 2024

Human error remains one of the leading causes of data breaches, with some studies claiming that it accounts for 88%-95% of all breaches. There are various types of human errors that can lead to data breaches, including but not limited to, using weak passwords, ignoring software updates, unintentionally sharing data, and falling for phishing scams. Since 2019, phishing scams have increased by over 150% per year. With the recent rise in artificial intelligence (AI) technology, the amount and success of phishing scams are expected to increase even more.

Credit: zapp2photo/stock.adobe.com

"Phishing" refers to the practice of sending fraudulent emails or other messages purporting to be from reputable individuals or companies to induce individuals to reveal personal information, to trick the user into clicking on a link to a malicious website or program, or to otherwise take advantage of the user. Traditional phishing scams involve sending one or more generic emails to as many individuals as possible, with the goal that some of them will fall victim to the fraud. Conversely, spear phishing involves selecting specific targets and crafting customized emails based on the target's position in order to maximize the phishing scheme's likelihood of success and potential return.

For example, a spear phishing email may target a company employee purporting to be from the company's IT department in an attempt to have the employee reveal their login credentials. Spear phishing's quality-over-quantity approach takes significantly more time and resources than traditional phishing but is substantially more likely to be successful. Recently, Facebook and Google lost over $100 million, less than half of which was recovered, when a threat actor determined that both companies used a certain Taiwanese vendor and sent fake invoices to employees impersonating the vendor. These spear phishing tactics may also be deployed directly against a company's vendors in order to leverage the vendor's access to the company's systems and comparatively minimal security.

AI, with its ability to analyze huge amounts of data in seconds, 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, check it for spelling or other errors, populate the "To" and "Subject" lines, and send it. Moreover, as AI has become more sophisticated, studies have shown that AI-generated emails are now indistinguishable from those written by humans. While phishing emails used to be plagued by typos like spelling mistakes or poor grammar due to the drafter's haste or lack of familiarity with the English language, which could in turn cause the recipient to become suspicious and detect the scam, AI-generated emails avoid these common errors. Additionally, AI tools can also analyze the results of traditional phishing to determine which emails were successful in order to improve future attempts.

AI's effect on spear phishing has been even more pronounced. Previously, spear phishing required threat actors to select the initial targets, extensively research that individual and/or their company, then use that information to craft an email or manufacture an entire scenario designed to defraud the target. This meant that threat actors were limited not by the number of viable targets, but by the time investment required for each attempt. AI, however, can automate each of these tasks and complete them nearly instantly, with varying levels of human oversight. Further, AI can be used to add to the authenticity of the resulting spear phishing attempt by, for example, leaving a fake voicemail. "Voice phishing" or "Vphishing" refers to the use of voice clips, such as publicly available clips of a person speaking at an event or conference, to credibly simulate their voice in a phone call or message. Scammers can use this technology to leave a convincing voicemail and make an accompanying email more believable or create a sense of urgency.

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. For example, HIPAA requires covered entities to maintain "reasonable and appropriate administrative, technical, and physical safeguards" for protected health information. Companies may also be contractually required to implement certain "reasonable" cybersecurity measures to protect against phishing and other threats. "Reasonable" is necessarily a fluid standard, considering the sensitivity of the data, the company's financial capabilities, potential threats, and other factors. Given the novelty of AI-assisted phishing, neither government agencies nor the courts have had the opportunity to weigh in on what is "reasonable" to combat more sophisticated AI-enhanced phishing attempts.

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.

At the end of the day, however, 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.

Kate A. Sherlock *is a partner in Archer & Greiner's Intellectual Property and Business Counseling Groups. She can be reached at ksherlock@archerlaw.com.*

Nicholas T. Franchetti is an associate with *Archer & Greiner's Business Litigation Group. He can be reached at nfranchetti@archerlaw.com.*