Cyberthreat Landscape for PEOs

Every spring in Washington, D.C., we reach peak bloom for the cherry blossoms that decorate the National Mall. Just as the setting around the tidal basin is constantly changing, so does the landscape for PEOs navigating our new AI-enhanced cyberthreat landscape. In 2025, there has been a notable uptick in phishing and voice based social engineering attacks around our industry. In both cases, the frequency of the attacks is less remarkable than the sophistication and convincing nature of the methods employed by cybercriminals.

With respect to phishing, the ability to train Large Language Models (LLMs) on the proper formatting for emails from specific companies has made it possible for threat actors to send emails without the telltale spelling and formatting errors that employees are trained to look for. Additionally, the use of LLMs allows cybercriminals to mimic a company's phraseology with enough accuracy that a casual reader won't think that anything is amiss. For example, a cybercriminal may not know what "PEO" means, but the utilization of a properly trained LLM will almost guarantee that they use the term correctly while trying to get you to click on a malicious link in a phishing email.

Sophisticated tools that generate voice (and increasingly visual) "deepfakes" are readily available. Like malicious emails, voice-based fraud can cut both ways. We must be vigilant in training our employees to look out for fraudsters pretending to be customers, but we also must create policies and consistent practices that protect our customers from cybercriminals pretending to be a PEO. For our employees, that means regular training and testing with increasing difficulty over time. To help the small and medium size business that we serve, it is imperative that PEOs adopt secure practices and "train" customers in the right way to do things, especially when interacting with a PEO.

See examples below

Avoid Email

Get out of the business of sending sensitive information over email. Adopt a secure file transfer tool for sharing sensitive data with third parties (including customers) and require your employees to use it.

Why: Training customers to expect requests for sensitive information via email is a goldmine for threat actors. Our customers are busy and working with limited resources. Sophisticated emails impersonating your PEO are now trivial to produce. If you train your customers to expect you to use email for transferring sensitive information, then their defenses will be lowered when a cybercriminal does the same thing.

Enhance Verification

Build enhanced verification processes for sensitive transactions like changing direct deposit account information.

Why: At the end of the day, cybercriminals want to steal money or assets they can sell for money (e.g., personal information). Phishing, voice impersonation, and all the other methodologies are just means to that end. Think of the ways in which a customer can impact where their money is deposited or how they share their sensitive information with you and build some sort of verification into those processes. It can be as simple as a verifying phone call to a known contact before changing bank account numbers in your system. One note on this example: email is ok for notifications of impending or recent changes, but you shouldn't use it as your sole verification method.

Implement MFA

Implement Multi-Factor Authentication (MFA) and require its use by employees and customers.

Why: MFA is the most effective tool available for preventing successful phishing attacks. It isn't perfect, but it is highly effective and relatively easy to implement. In 2025, it is a basic requirement for any business in our industry. If you already have MFA implemented, keep in mind that it can be used for more than just logins. An additional MFA prompt is a great verification method for the example above.

As always, our people are the largest attack vector for threat actors looking to gain access to our systems. Train and test your employees and implement thoroughly tested security tools (like MFA), but don't forget to train your customers to transact with you in a secure manner and, most importantly, make sure they expect you to do the same.

NAPEO

National Association of Professional Employer Organizations

707 North Saint Asaph Street, Alexandria, VA 22314 • 703/836-0466