AGH CPAs & ADVISORS

ALERT: Employers could be responsible for damages in phishing scams

August 8, 2018

With the ever increasing occurrence of "phishing" attacks, employers can no longer ignore the risk it bears for their employees and overall business. According to a recent federal court decision, an employer could face legal action and be forced to pay financial damages for an employee's mistake.

This is precisely what happened to a North Carolina company when an employee received an email that appeared to be from a supervisor. The email requested W-2 tax information for the company's employees for verification purposes. The employee sent the supposed supervisor an unencrypted file containing the requested information. Despite what was likely an employee acting with the best of intentions, the employee was fooled into sharing the personal information (including Social Security numbers) of more than 200 employees with a cybercriminal.

It is common for these types of phishing emails to occur during month-end when employees are busy and the request seems timely and legitimate.

Several employees sued, and a federal court determined that the email response, despite being made under false pretenses, was intentionally made. The court's reasoning noted the distinction between a breach and a disclosure indicating the following:

- Data breach: "wherein a hacker infiltrated the defendant's computer systems and stole the plaintiffs' information"
- Data disclosure: "wherein the defendant intentionally responded to an email request with an unencrypted file containing highly sensitive information regarding its current and former employees"

Under the rationale of intentional disclosure of confidential employee information, the court allowed the employees to seek treble damages.

Treble damages – a recovery of three times the amount of actual financial losses suffered.

How to protect your organization from phishing threats

In the North Carolina case, the Court noted that the company failed to provide "even the most basic of security measures" that could have prevented the disclosure.

Phishing exploits human weaknesses even more than technical vulnerabilities. If you want to effectively protect your network from phishing attacks, address the human source of the problem. This can be addressed first and foremost through educating and training your employees. Most employees are willing to help, but won't be able to if they don't know how.

At AGH, our technology professionals are equipped with the tools necessary to help educate your staff on the dangers of phishing and reduce their susceptibility to attacks, as well as how to improve their handling of sensitive information. Our training addresses your employees' vulnerabilities and leaves them better prepared to protect your information assets.

Learn more about phishing attacks and how to prevent them at aghlc.com/phishing

Additionally, consider consulting with experts at AGH before a cyber crisis happens. An incident response plan and mitigation efforts can help your company recover more quickly and with less disruption should a cyber security incident occur. Finally, the AGH team is prepared to assist in emergency situations as well. Notify us immediately should you find your organization's data has been compromised.

AGH's professionals have a proven record of helping organizations keep their information secure and can educate leaders on their organization's information security by performing comprehensive risk assessments and system evaluations. To get started, contact Brian Johnson, senior vice president of technology services, at Brian.Johnson@aghlc.com or 316.291.4107.