STRADLEY RONON

Data Breach Alert

A Publication of the Stradley Ronon
Data Breach Practice

WWW.STRADLEY.COM

MARCH 2, 2017

Stradley Ronon Stevens & Young, LLP
2005 Market Street
Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
New York
New Jersey
Illinois
Delaware

Jana M. Landon

Peter Bogdasarian

Tax Season is Spear Phishing Season

As the weather warms in the mid-Atlantic and accountants' thoughts turn to taxes, so too do the phishers. Scammers who specialize in tax refund fraud have returned to a favorite trick from 2016: spoofing emails from C-suite executives at target organizations, requesting human resources and accounting departments for employee W-2 information by email, then using that information to file false tax returns. A type of attack like this, where the apparent source of the email is a prominent individual within the recipient's own company is known as "spear phishing," a variant on the ever-popular fake emails from "trusted" sources that ask you to provide confidential information.

Employees in human resources and accounting departments are normally identified by the fraudsters through social networking sites such as LinkedIn. While the scammers rake in their stolen money, the target organization is left to contend with the aftermath, which inevitably involves state (and sometimes federal) data breach laws and having to rebuild trust with its employees and customers. This problem is widespread – the IRS issued an alert in late January warning companies that payroll and human resources departments are again being targeted by criminals this year seeking W-2 information.

The success of spear phishing depends upon three things: the email "sender" must appear to be a known and trusted individual, there is information within the message that supports its validity (e.g., that the CEO is working on a benefits package for employees), and the request the individual makes seems to have a logical basis. The best weapon in the fight against these scammers is education and awareness. Employees should be educated on phishing fraud with a special attention to authority-based requests that call for the transmittal of confidential information by email or request password information.

Education, in the context of all types of phishing fraud, typically focuses on several areas of security awareness: (a) having a healthy skepticism about email; (b) being able to identify the difference in a reply-to address from the spoofed address of the apparent sender (after all, the phisher cannot capture the information unless it is set to an address he controls); (c) the importance of taking extra precautions to safeguard confidential information (experience shows that picking up the phone and making a call to verify the email would often have prevented the breach); and (d) support from the organization's information security and information technology departments to work to prevent spear phishing messages from reaching employee mailboxes.

Last, if your company experiences a spear phishing attack, it is important to move quickly to minimize losses. Engage counsel immediately to guide you through the murky waters of reporting obligations, law enforcement notification, possible forensic investigation and employee notification.

Phishing campaigns can happen at any time, but are on the uptick during tax season. Alert your staff now that all emails requesting confidential information for employees should be verified. Be careful out there!