April, 7, 2016

Don’t Let Hackers Get Your Tax Refund

What if I told you there are people out there who would love to do your taxes for you, and no upfront cost, without requiring any work on your part? In fact, you won’t even have to know they’re doing it – they’ll take care of it all on their own, no questions asked.

Sounds like a good deal, right?

Well, unfortunately, these people are known as cyber thieves, and they certainly don’t just want to do you a favor. They want to steal your refund after filing fraudulent taxes using your personal information.

With the tax deadline fast approaching, protect yourself from theft by keeping an eye out for suspicious emails. Over the past 12 months, we have seen a significant increase in what is called a “spear-phishing attack,” in which an employee of a company will receive a fraudulent email from a hacker impersonating a company executive, usually a CEO. This phishing email typically contains a request to transfer funds to a bank account or routing number that has been set up by the hacker. The unsuspecting employee, wanting to comply with a request from a superior, releases the funds to the fraudulent account, and the money virtually disappears.

Hackers are becoming more creative in their approach to these phishing schemes. Recently, there have been multiple instances of an employee, typically in human resources, receiving an email from what appears to be the CEO urgently requesting W-2 information for all employees of the company.

The unsuspecting employee obliges, releasing countless records of highly sensitive personal information of the employees. This information can be used for a variety of purposes including filing fraudulent tax returns under the employees’ names and receiving the refund money associated with these returns.

Still, obtaining sensitive personal information is actually becoming more useful to hackers than fraudulent funds transfers. Not only can employees be subject to identity theft as a result of this hacking scheme, but their legitimate tax filings may ultimately be rejected by the IRS.

In addition to being aware and wary of these tactics, we strongly recommend purchasing Cyber/Privacy Liability and Crime insurance for these types of breaches. It is also critically important that each company be proactive in examining and re-examining their cyber security protocols. This method of spear-phishing does not necessarily involve a highly sophisticated

hacker, but instead an unsuspecting employee cooperating with the request of a “senior officer.”

The following risk control measures are examples of steps that can be taken to thwart a spear-phishing attack:

1) Provide training seminars to staff members, alerting them of issues and schemes such as this one.

2) All employees, and especially those in human resources or payroll departments, should be trained to confirm requests of this type before releasing any information. For example, calling the CEO to confirm whether or not he or she actually requested the information is a quick and easy way to legitimize a request of this nature.

3) Be mindful of who is requesting the information. In many instances it would be odd for the CEO or another executive of the company to suddenly request all W-2 information of employees, especially if this is a practice that has not been done in the past.

If you have any questions related to this issue, or would like to discuss insurance or risk control measures and remedies, please contact your account executive team.

connerstrong.com 877-861-3220 news@connerstrong.com Change My Preferences

CONNER STRONG & BUCKELEW

INSURANCE | RISK MANAGEMENT | EMPLOYEE BENEFITS