PUBLICATION

Tax Season Becomes "Spear Phishing" Season for Cybercriminals

January 13, 2017

Imagine this scenario. Your HR team receives an email from your CEO: "I want you to send me W-2s of employees' wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment." They hurry to get the boss the materials she needs, and by the time they begin to wonder why the CEO would ask for every employee's W-2 to be sent to her via email, the cybercriminal who actually sent the spear phishing email that HR responded to probably will have had every one of those employees' personal data for days – or weeks.

Last year, at least 68 U.S. companies found themselves in this exact situation – victims of "W-2 spear phishing" attacks.

Spear phishing is a dead-simple, yet ruthlessly effective, form of cyberattack where the attacker sends a target email that appears to be from a trusted source, yet on closer inspection actually comes from an illegitimate domain. Thus, HR departments who think that they are sending confidential information in response to a request from "TheBoss@BigCompany.com" are actually sending that information to an attacker whose email is "TheBoss@BigCornpany.com."

If you had to read that last part twice before you noticed that the two email addresses are different, you can understand why the attacks at those 68 organizations (as well as an unknown number of others that may not have reported) occurred during the 2016 tax season. These attacks resulted in the disclosure of the personal information of thousands of employees that then was used (among other nefarious acts) to file fraudulent tax returns so that the attackers could steal the tax refunds.

And no industry or sector was immune; breaches occurred at a large state university, a computer hardware manufacturer, a tech start-up, health care companies, retail companies, construction firms, wholesale suppliers and more. By the time the IRS sent an alert on March 1, 2016, much of the damage had already been done.

In preparing for the 2017 tax season, your organization needs to be vigilant not only in the event that "phishing season" reopens, but also to be mindful that this year's novel cyberattack will probably look different. Thus, be prepared to protect personal and confidential data generally, keeping in mind several best practices:

- **Personal information is not sent via unsecured email.** Ever. When this message becomes part of your organization's culture, emails that request personal information will automatically raise alarm bells.
- **Challenge and confirm.** Because employees may be nervous to tell higher-ups "no," or be all too eager to "be helpful" to someone they think is a high-level executive, the leadership should communicate that they will expect that their identity will need to be confirmed for any unusual requests and that they don't take it personally.
- **Segregate data and control user access.** Determine where personal and confidential information is kept and who has access to it. If personal and confidential information is comingled on systems with day-to-day business records, move and secure that data. And if user access is misaligned with job function, modify access as soon as possible.

- **Proper training.** Once the access is limited to only those who need it, make sure that those individuals have proper training on security and confidentiality.

And if you do find yourself the victim, don't panic, but act quickly; state privacy laws may require action within hours of the discovery. Baker Donelson's Privacy and Information Security Group is available to assist with any questions or legal advice in connection with suspected data security incidents and to give counsel on the steps you need to take next.

Please contact any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team to assist with any questions or legal advice in connection with data protection or other privacy and security issues.