New Phishing Scam Involving Company W-2s

Posted At : March 11, 2016 11:47 AM | Posted By : Admin
Related Categories: Your Business, Security

Your company bookkeeper or outside accountant receives a seemingly innocuous email from the CEO, owner, or other "high up" person in the organization asking for a copy of all the 2015 W-2s in pdf form. Simple enough - just one of the many things that need to be responded to every day. Except this one isn't innocuous. It's a trap to capture your employee's social security numbers. And unfortunately, because of its deceptive simplicity, it's been successful in a few places.

"Can't happen here." or "We are way to small." No such thing. No organization is immune and even the best anti-malware products may not be able to keep up with every single instance of this Scam. In the last couple of weeks, we have seen instances with some of our clients where this exact Phishing Scam has been identified Fortunately, most people are vigilant and aware. They asked their superiors to confirm the request and stopped the issue then and there.

Below is a release from the IRS outlining this issue in more detail. Bottom line is simple: You can't be too careful with important company information. Always ask questions and independently doublecheck those kinds of requests.

IR-2016-34, March 1, 2016

WASHINGTON — The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees.

The IRS has learned this scheme — part of the surge in phishing emails seen this year — already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives.

"This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees."

IRS Criminal Investigation already is reviewing several cases in which people have been tricked into sharing SSNs with what turned out to be cybercriminals. Criminals using personal information stolen elsewhere seek to monetize data, including by filing fraudulent tax returns for refunds.

This phishing variation is known as a "spoofing" email. It will contain, for example, the actual name of the company chief executive officer. In this variation, the "CEO" sends an email to a company payroll office employee and requests a list of employees and information including SSNs.

The following are some of the details contained in the e-mails:

- Kindly send me the individual 2015 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review.

- Can you send me the updated list of employees with full details (Name, Social Security Number, Date of Birth, Home Address, Salary).

- I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.

The IRS recently renewed a wider **consumer alert** for e-mail schemes after seeing an approximate 400 percent surge in phishing and malware incidents so far this tax season and other reports of scams targeting others in a wider tax community.

The emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. The phishing schemes can ask taxpayers about a wide range of topics. E-mails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information.

The IRS, state tax agencies and tax industry are engaged in a public awareness campaign — Taxes. Security. Together. — to encourage everyone to do more to protect personal, financial and tax data. See **IRS.gov/taxessecuritytogether**or **Publication 4524** for additional steps you can take to protect yourself.