Published on *The National Law Review* https://natlawreview.com

IRS Issues Warning About W-2 Cyber-Scams, Especially for Schools, Nonprofits and Tribal Organizations

Article By:

Workplace Safety and Health

On February 2, 2017, the ***Internal Revenue Service*** issued a warning to all employers regarding the resurgence of a W-2 based cyber scam. The scam, which targets the corporate world during tax season, is currently "spreading to other sectors, including school districts, tribal organizations and nonprofits." (irs.gov/news-events).

This cyber-scam is simple, but highly successful. It consists of an e-mail sent to an employee in the Human Resources or Accounting department from an executive within the organization. Both the TO and FROM e-mail addresses are accurate internal addresses, as are the sender's and recipient's names. The e-mail requests that the recipient forward the company's W-2 forms, or related data, to the sender. This request aligns with the job responsibilities of both parties to the email.

Despite appearances, the e-mail is a fraud. The scammer is "spoofing" the executive's identity. In other words, the cyber-criminal assumes the identity and e-mail address of the executive for the purpose of sending what appears as a legitimate request. The recipient relies on the accuracy of the sender's e-mail address, coupled with the sender's job title and responsibilities, and forwards the confidential W-2 information. The forwarded information goes to a hidden e-mail address controlled by the cyber-criminal.

When successful, the cyber-criminal obtains a trove of sensitive employee data that may include names, dates of birth, addresses, salary information, and social security numbers. This information is used to file fake tax returns and requests for tax refunds and/or sold on the dark web to perpetrators of identity theft.

The IRS gives examples of these W-2 e-mail requests on its website:

- "Kindly send me the individual 2016 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 2016. I

need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap."

These cyber-scams, known as business email compromise (BEC) attacks, or CEO spoofing, are a form of 'spear phishing.' Spear phishing targets a specific victim using personal or organizational information to elicit the victim's trust. The cyber-criminal obtains and uses information such as personal and work e-mail addresses, job titles and responsibilities, names of friends and colleagues, personal interests, etc. to lure the victim into providing sensitive or confidential information. Quite often, the scammers cull this information from social media, LinkedIn, and corporate websites. The method is both convincing and highly successful.

While an organization can use firewalls, web filters, malware scans or other security software to hinder spear phishing, experts agree the best defense is employee awareness. This includes ongoing security awareness training for all levels of employees, simulated phishing exercises, internal procedures for verifying transfers of sensitive information, and reduced posting of personal information on-line.

Although simple, the W-2 e-mail scam can have a devastating impact on an organization and its employees. And, although equally simple, employee awareness can help prevent it.

Instances of W-2 or similar attacks should be reported to the IRS at phishing@irs.gov and the Internet Crime Complaint Center of the FBI.

Mary Costigan is the author of this article.

National Law Review, Volume VII, Number 39