

Don't Get Hooked! W-2 Phishing Scams on the Rise During Tax Season

by Melissa Raphan and Jillian Kornblatt

Tax season can be a trying time of the year for any employer, but even more so now. As HR Departments across the country are working hard to distribute W-2 forms to employees, cybercriminals are using increasingly sophisticated techniques to con staff employees into disclosing sensitive personally identifiable information ("PII") contained in those W-2s, including names, addresses, and social security numbers of employees. These efforts are reaching epidemic proportions as more and more cybercriminals target medium to smaller sized companies, and previously untapped sectors like school districts, tribal organizations, and nonprofits.

Cybercriminals use a technique called "phishing" to gain access to company W-2s. Phishing can take any number of different pathways. Here's how it typically works: a cybercriminal will use easily accessed public information about individuals in management positions in a company, disguise an email address to appear to be from a company executive, and then send it to a targeted mid-level staff member in HR, Finance or Accounting to request a list of employees and their associated W-2 forms. Phishing scams are so prevalent that the Internal Revenue Service ("IRS") provided an emergency notice to all economic sectors, instructing entities to be particularly vigilant. See IRS, *Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others*, [irs.gov](https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others) (Feb. 2, 2017), <https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others>.

Often these cons will take place on Friday afternoon, as employees may be distracted with week-ending tasks. If successful, the cybercriminals will use the W-2's to file false tax returns over the weekend, and by the time the crime is discovered on Monday it may be too late to prevent the theft. All too often, the only step left for the employer to take is to notify its' employees after the fact under a cumbersome system of individual breach notification laws from 48 different states, and coach them through the process of notifying credit monitoring agencies, the IRS, and the Federal Trade Commission ("FTC"). At a minimum, employers will offer credit monitoring to affected employees; as

Related People

- Melissa Raphan
- Jillian Kornblatt

Related Capabilities

- Privacy & Social Media
- Telecommunications
- Labor & Employment

the limits of that protection are becoming increasingly obvious, more effective – and expensive – identity theft protection services are increasingly the norm.

Unlike most other cyber crimes, W-2 scams can be prevented. There are a few simple tips each employer can follow to minimize that risk:

- *Education and training.* Almost everyone has heard about the W-2 scams, but companies continue to fall prey to cleverly disguised spoof emails if vigilance is not top-of-mind. Even simple reminders to key employees with access to W-2 data that “it’s that time of year” can be effective.
- *Limit access to sensitive employee information (not just W-2s).* Use the current threat as a catalyst to rethink who has access to what information, and why. This is just good information governance, but it is easily overlooked.
- *Consider strict limits on which executives can request access to, much less copies of, sensitive employee information.*
- *Even where access is required, consider two-factor authentication whenever sensitive employee information is involved.*
- *Restrict any bulk transfer of sensitive employee information.*
- *Institute regular training on phishing scams.* The FBI estimates that even well-trained employees may fail to spot fake emails and attachments between 10-25% of the time. The time, expense, and – let’s be honest, headache – of employee training pales in comparison to the consequences of a scammed disclosure of sensitive employee information.

Unfortunately, no firewall is perfect, no detection system is foolproof, and no amount of training or vigilance can be 100% effective. If you should fall victim to a W-2 scam, or any other cyber attack, we have extensive experience in rapid response assistance, including lightning-fast early warning procedures designed to minimize the ability of cyber criminals to use purloined information, and a deep bench experienced in providing notifications to employees compromised by the breach, contacting the State Attorneys General as required under numerous state breach statutes, as well as state tax authorities and the IRS, and a well-developed relationship with the FBI when its assistance may prove helpful.