

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Feb. 02, 2017



The IRS, state tax agencies and the tax industry issued an urgent alert today to all

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns. We need everyone's help to turn the tide against this scheme," said IRS Commissioner John Koskinen.

When employers report W-2 thefts immediately to the IRS, the agency can take steps to help protect employees from tax-related identity theft. The IRS, state tax agencies and the tax industry, working together as the Security Summit, have enacted numerous safeguards in 2016 and 2017 to identify fraudulent returns filed through scams like this. As the Summit partners make progress, cybercriminals need more data to mimic real tax returns.

Here's how the scam works: Cybercriminals use various spoofing techniques to disguise an email to make it appear as if it is from an organization executive. The email is sent to an employee in the payroll or human resources departments, requesting a list of all employees and their Forms W-2. This scam is sometimes referred to as business email compromise (BEC) or business email spoofing (BES).

The Security Summit partners urge all employers to be vigilant. The W-2 scam, which first appeared last year, is circulating earlier in the tax season and to a broader cross-section of organizations, including school districts, tribal casinos, chain restaurants, temporary staffing agencies, healthcare and shipping and freight. Those businesses that received the scam email last year also are reportedly receiving it again this year.

Security Summit partners [warned of this scam's reappearance](#) last week but have seen an upswing in reports in recent days.

### **New Twist to W-2 Scam: Companies Also Being Asked to Wire Money**

In the latest twist, the cybercriminal follows up with an "executive" email to the payroll or comptroller and asks that a wire transfer also be made to a certain

account. Although not tax related, the wire transfer scam is being coupled with the

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Organizations receiving a W-2 scam email should forward it to [phishing@irs.gov](mailto:phishing@irs.gov) and place "W2 Scam" in the subject line. Organizations that receive the scams or fall victim to them should file a complaint with the Internet [Crime Complaint Center](#) (IC3,) operated by the Federal Bureau of Investigation.

Employees whose Forms W-2 have been stolen should review the recommended actions by the Federal Trade Commission at [www.identitytheft.gov](http://www.identitytheft.gov) or the IRS at [www.irs.gov/identitytheft](http://www.irs.gov/identitytheft). Employees should file a Form 14039, Identity Theft Affidavit, if the employee's own tax return gets rejected because of a duplicate Social Security number or if instructed to do so by the IRS.

The W-2 scam is just one of several new variations that have appeared in the past year that focus on the large-scale thefts of sensitive tax information from tax preparers, businesses and payroll companies. Individual taxpayers also can be targets of phishing scams, but cybercriminals seem to have evolved their tactics to focus on mass data thefts.

## Be Safe Online

In addition to avoiding email scams during the tax season, taxpayers and tax preparers should be leery of using search engines to find technical help with taxes or tax software. Selecting the wrong "tech support" link could lead to a loss of data or an infected computer. Also, software "tech support" will not call users randomly. This is a scam.

Taxpayers searching for a paid tax professional for tax help can use the IRS [Choosing a Tax Professional lookup tool](#) or if taxpayers need free help they can review the [Free Tax Return Preparation Programs](#). Taxpayers searching for tax software can use Free File, which offers 12 brand-name products for free, at [www.irs.gov/freefile](http://www.irs.gov/freefile). Taxpayer

or tax preparers looking for tech support for their software products should go

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2024 Firmworks, LLC. All rights reserved