

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

operating officers, school executives or others in positions of authority. Using a technique known as business email compromise (BEC) or business email spoofing (BES), ...

Jan. 17, 2018



U.S. businesses need to watch out for a Form W-2 phishing scam that made victims of hundreds of organizations and thousands of employees last year.

The IRS says the Form W-2 scam has emerged as one of the most dangerous phishing emails in the tax community. During the last two tax seasons, cybercriminals tricked

payroll personnel or people with access to payroll information into disclosing

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

By alerting employers now, the IRS and its partners in the [Security Summit effort](#) hope to limit the success of this scam in 2018. The IRS last year also created a new process by which employers should report these scams. There are steps the IRS can take to protect employees, but only if the agency is notified immediately by employers about the theft.

Here's how the scam works: Cybercriminals do their homework, identifying chief operating officers, school executives or others in positions of authority. Using a technique known as business email compromise (BEC) or business email spoofing (BES), fraudsters posing as executives send emails to payroll personnel requesting copies of Forms W-2 for all employees.

The Form W-2 contains the employee's name, address, Social Security number, income and withholdings. Criminals use that information to file fraudulent tax returns, or they post it for sale on the Dark Net.

The initial email may be a friendly, "hi, are you working today" exchange before the fraudster asks for all Form W-2 information. In several reported cases, after the fraudsters acquired the workforce information, they immediately followed that up with a request for a wire transfer.

In addition to educating payroll or finance personnel, the IRS and Security Summit partners also urge employers to consider creating a policy to limit the number of employees who have authority to handle Form W-2 requests and that they require additional verification procedures to validate the actual request before emailing sensitive data such as employee Form W-2s.

If the business or organization victimized by these attacks notifies the IRS, the IRS can take steps to help prevent employees from being victims of tax-related identity theft. However, because of the nature of these scams, some businesses and

organizations did not realize for days, weeks or months that they had been

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

- Include the following:
- Business name
- Business employer identification number (EIN) associated with the data loss
- Contact name
- Contact phone number
- Summary of how the data loss occurred
- Volume of employees impacted

Businesses and organizations that fall victim to the scam and/or organizations that only receive a suspect email but do not fall victim to the scam should send the full email headers to phishing@irs.gov and use "W2 Scam" in the subject line.

Employers can learn more at [Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers](#).

Employers should be aware that cybercriminals' scams constantly evolve. Finance and payroll personnel should be alert to any unusual requests for employee data.

Income Tax • Taxes

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