IRS

Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers

As the Internal Revenue Service, the state tax agencies and the tax industry make progress combatting identity theft, cybercriminals need more data to impersonate real taxpayers and file fraudulent returns for refunds.

Currently, a particularly dangerous email scam is circulating. Here's how it 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).

Because time is critical, the IRS has created avenues for businesses and payroll service professionals to report if they lost data to this scam or if they only received the email without falling victim. If your company did not fall victim, see how to report the scam email to the IRS.

How to report a data loss related to the W-2 scam

If notified quickly after the loss, the IRS may be able to take steps that help protect your employees from tax-related identity theft. Ways to contact the IRS* about a W-2 loss include

- Email dataloss@irs.gov to notify the IRS of a W-2 data loss and provide your contact information listed below so that we may call you. In the subject line, type "W2 Data Loss" so that the email can be routed properly. Do not attach any employee personally identifiable information (PII) data.
  a. Business name
  b. Business employer identification number (EIN) associated with the data loss
  c. Contact name

d. Contact phone number
e. Summary of how the data loss occurred
f. Volume of employees impacted

*The IRS doesn't ***initiate*** contact with taxpayers by email, text messages or social media channels to request personal or financial information. Any contact from the IRS will be in response to a contact initiated by you. Cybercriminals, when they learn of a new IRS process, often create false IRS web sites and IRS impersonation emails.

How to report data loss to state tax agencies

- Any breach of personal information could have an effect on the victim's tax accounts with the states as well as the IRS. You should email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.

How to report data loss to other law enforcement officials

- Businesses/payroll service providers should file a complaint with the FBI's Internet Crime Complaint Center (IC3)
- Businesses/payroll service providers may be asked to file a report with their local law enforcement agency

What to tell your employees about a Form W-2 data loss

Cybercriminals who successfully steal Forms W-2 immediately attempt to monetize their thefts. Criminals may immediately attempt to file fraudulent tax returns claiming a refund. Or, they may sell the data on the Internet's black market sites to others who file fraudulent tax returns or use the names and SSNs to create other crimes. Here is some guidance to share with your employees:

1. Review Taxpayer Guide to Identity Theft
2. Share IRS Publication 5027 PDF, Identity Theft Information for Taxpayers, with employees and direct them to the "Steps for Identity Theft Victims" which includes:
   - Contacting one of the three credit bureaus to place a "fraud alert" on their account; they may consider placing a "credit freeze" which offers more protection.
   - File a complaint with the Federal Trade Commission, the lead federal agency on identity theft issues.
   - Review FTC www.identitytheft.gov information for additional steps to recover from identity theft.
3. The FTC also offers guidance to businesses on how to inform employees of the incident and additional steps businesses may take. See Data Breach Response: A Guide for Business.
4. Share IRS Publication 4524 PDF, Security Awareness for Taxpayers, with your employees

How to report receiving the W-2 phishing email

If your business received the email but did NOT fall victim to the scam, forward the email to the IRS. The IRS needs the email header from the phishing email for its investigation, which means you must do more than just forward the email to phishing@irs.gov. Here's what to do with the W-2 email scam:

1. The email headers should be provided in plain ASCII text format. Do not print and scan
2. Save the phishing email as an email file on your computer desktop
3. Open your email and attach the phishing email file you previously saved
4. Send your email containing the attached phishing email file to phishing@irs.gov. Subject Line: W2 Scam. Do not attach any sensitive data such as employee SSNs or W-2s.
5. File a complaint with the Internet Crime Complaint Center (IC3,) operated by the Federal Bureau of Investigation.

Page Last Reviewed or Updated: 24-Feb-2021