Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 February 2018

Alert Number

I-022118-PSA

Increase in W-2 Phishing Campaigns

Beginning in January 2017, IRS's Online Fraud Detection & Prevention (OFDP), which monitors for suspected IRS-related phishing emails, observed an increase in reports of compromised or spoofed emails requesting W-2 information. Sometimes these requests were followed by or combined with a request for an unauthorized wire transfer.

The most popular method remains impersonating an executive, either through a compromised or spoofed email in order to obtain W-2 information from a Human Resource (HR) professional within the same organization.

Individual taxpayers may also be the targeted, but criminals have evolved their tactics to focus on mass data thefts.

This scam is just one of several new variations of IRS and tax-related phishing campaigns targeting W-2 information, indicating an increase in the interest of criminals in sensitive tax information.

How to report a data loss related to IRS related to a 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. To contact the IRS about a W-2 loss, email IRS at dataloss@irs.gov and provide the information listed below so the IRS can contact you. In the subject line, type "W-2 Data Loss" so that the email can be routed properly. Do not attach any employee personally identifiable information (PII) data.

Provide the following information in your email:

1. Business name
2. Business employer identification number (EIN) associated with the data loss
3. Contact name
4. Contact phone number
5. Summary of how the data loss occurred
6. Volume of employees impacted

Note: 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. Criminals, 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) at ic3.gov
- Businesses/payroll service providers may be asked to file a report with their local law enforcement agency

How to report W-2 phishing emails to IRS

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.

There are various ways to view and save an email header depending on your email client program or web service. Please research the method that corresponds with your program or service.

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: W-2 Scam
5. Do not attach any sensitive data such as employee SSNs or W-2s
6. File a complaint with the Internet Crime Complaint Center (IC3) at ic3.gov

Recommendations and Best Practices

The key to reducing the risk from W-2 phishing scams and BEC is to understand the criminals' techniques and deploy effective mitigation processes. There are various methods to reduce the risk of falling victim to this scam and subsequently disclosing sensitive information or executing a fraudulent wire transfer.

Some of these methods include:

- Limit the number of employees within a business who have the authority to approve and/or conduct wire transfers and handle W-2 related requests or tasks
- Use out of band authentication to verify requests for W-2 related information or wire transfer requests that are seemingly coming from executives. This may include calling the executive to obtain verbal verification, establishing a phone Personal Identification Number (PIN) to verify the executive's identity, or sending the executive via text message a one-time code and a phone number to call in order to confirm the wire transfer request
- Verify a change in payment instructions to a vendor or supplier by calling to verbally confirm the request. The phone number should not come from the electronic communication, but should instead be taken from a known contact list for that vendor

- Maintain a file, preferably in non-electronic form, of vendor contact information for those who are authorized to approve changes in payment instructions
- Delay the transaction until additional verifications can be performed such as having staff wait to be contacted by the bank to verify the wire transfer
- Require dual-approval for any wire transfer request involving one or more of the following:
    - A dollar amount over a specific threshold
    - Trading partners who have not been previously added to a "white list" of approved trading partners to receive wire payments
    - New trading partners
    - New bank and/or account numbers for current trading partners
    - Wire transfers to countries outside of the normal trading patterns

To address compromised domains it is recommended that, if possible, affected parties contact the appropriate service providers to report the activity and file a complaint with the Internet Crime Complaint Center (IC3) at ic3.gov.

Contact Information

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is the industry forum for collaboration on critical security threats facing global financial services sectors.

- FS-ISAC encourages member institutions to report any observed fraudulent activity through the FS-ISAC submission process and to login at fsisac.com. This reporting can be done with attribution or anonymously and will assist other members and their customers to prevent, detect and respond to similar activity. Anyone experiencing this activity is encouraged to reach out to the FS-ISAC SOC at mailto:soc@fsisac.us or call (877) 612-2622, prompt 2
- Employers who receive or fall victim to the W-2 scam should review guidance at Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers. For general questions, visit http://www.irs.gov/identitytheft
- All incidents, successful and attempted, should be reported to the Internet Crime Complaint Center at ic3.gov

Appendix

(IR-2016-34) https://www.irs.gov/uac/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w2s

(IR-2017-10) https://www.irs.gov/uac/newsroom/irs-states-and-tax-industry-renew-alert-about-form-w2-scam-targeting-payroll-human-resource-departments

(IR-2017-20) - https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others

(IR-2017-130) - https://www.irs.gov/newsroom/dont-take-the-bait-step-6-watch-out-for-the-w-2-email-scam

(IR-2018-8) - https://www.irs.gov/newsroom/irs-states-and-tax-industry-warn-employers-to-beware-of-form-w-2-scam-tax-season-could-bring-new-surge-in-phishing-scheme