Norton by Symantec | LifeLock

Tax Fraud & Phishing Scams

In order to file a U.S. tax return, identity thieves only need a name, Social Security number and date of birth.

FORM W-2 SCAM

Cybercriminals pose as a company executive in an email to payroll or human resources and request copies of Forms W-2 for all employees and even use an executive's signature block in the email to increase legitimacy. The initial email to the employee may be a simple but typically include language such as:

> *"Kindly send me the individual 2017 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review."*
>
> *"I want you to send me the list of W-2 copy of employee's wage and tax statement for 2017. I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap."*

During the last two filing seasons, cybercriminals have targeted all types of employers, including large and small businesses, public schools and universities, hospitals, tribal governments, and charities. For this reason, companies should take steps to educate their employees on how to help safeguard employee personal information.

Regardless of the phishing method, the IRS has recommended a number of basic steps all employers should take—whether it be a small tax preparer or a large business:

- Notify the IRS of all suspicious tax-related phishing emails (phishing@irs.gov).
- Educate all employees about phishing emails and train them to not click on pop-ups or suspicious links.
- Use strong, unique passwords.
- Never take an email from a familiar source at face value.
- Consider verbal confirmation by phone with the sender of an email before sending further information or accessing links or attachments.
- Consider limiting those employees who handle Form W-2 requests and requiring additional verification procedures before emailing forms.

$2.5B

According to the 2017 IRS Criminal Investigation annual Report, the IRS identified $2.5 billion in tax fraud.[1]

An identity (name, SSN, DOB) can be bought on the dark web for a low price and used by thieves for a range of threats.[2]

W-2

W-2 records can be bought on the dark web and could be used to commit tax refund fraud.[3]

4X

4x as many organizations were scammed into giving out their W-2 records in 2017 compared to 2016.[4]

1811

According to the 2017 IRS Criminal Investigation Division, 1811 investigations were initiated for tax crimes.[1]

400%

From the 2015 to 2016 tax season, the IRS reported an estimated 400% increase in phishing and malware incidents.[4]

29%

29 percent of 2016 consumers reported that their data was used to commit tax fraud.[5]

No one can prevent all identity theft.

[1] https://www.irs.gov/pub/foia/ig/ci/2017_criminal_investigation_annual_report.pdf
[2] 2017 Symantec Internet Security Threat Report
[3] IRS, "Don't Take the Bait, Step 6: Watch Out for the W-2 Email Scam", August 15th, 2017.
[4] IRS, "Consumers Warned of New Surge in IRS E-mail Schemes during 2016 Tax Season", February 18, 2016.
[5] https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints