exchange, all of an organization's Forms W-2 for their employees may be in the hands of cybercriminals. This puts workers at risk for tax-related identity theft.

Dec. 07, 2018

As the 2019 tax season approaches, the IRS, state tax agencies and the nation's tax industry joined together to warn small businesses to be on-guard against a growing wave of identity theft and W-2 scams.

Small business identity theft is big business for identity thieves. Just like individuals, businesses may have their identities stolen and their sensitive information used to open credit card accounts or used to file fraudulent tax returns for bogus refunds. Employers also hold sensitive tax data on employees, such as Form W-2 data, which also is highly valued by identity thieves.

"Identity theft can be devastating to small businesses, and the IRS continues to see instances where cybercriminals are targeting these groups to obtain sensitive

employee information that can be used to file fake tax returns," said IRS

business-related identity theft and scams.

Identity thieves have long made use of stolen Employer Identification Numbers (EINs) to create fake Forms W-2 that they would file with fraudulent individual tax returns. Fraudsters also used EINs to open new lines of credit or obtain credit cards. Now, they are using company names and EINs to file fraudulent returns.

The IRS has identified an increase in the number of fraudulent Forms 1120, 1120S and 1041 as well as Schedules K-1. The fraudulent filings apply to partnerships as well as estate and trust forms.

Businesses, partnerships and estate and trust filers should be alert to potential identity theft and contact the IRS if they experience any of these issues:

- Extension to file requests are rejected because a return with the Employer Identification Number or Social Security number is already on file;
- An e-filed return is rejected because a duplicate EIN/SSN is already on file with the IRS;
- An unexpected receipt of a tax transcript or IRS notice that doesn't correspond to anything submitted by the filer.
- Failure to receive expected and routine correspondence from the IRS because the thief has changed the address.

Complete trusted customer questions

The IRS, state tax agencies and software providers also share certain data points from returns, including business returns, that help identify a suspicious filing. The IRS and states also are asking that business and tax practitioners provide additional information that will help verify the legitimacy of the tax return.

These “know your customer” procedures are being put in place and include the

tax forms?

Sole proprietorships that file Schedule C and partnerships filing Schedule K-1 with Form 1040 also will be asked to provide additional information items, such as a driver’s license number. Providing this information will help the IRS and states identify suspicious business-related returns.

For small businesses looking for a place to start on security, the Federal Trade Commission maintains a Protecting Small Business page which includes a series on cybersecurity and a Cybersecurity for Small Business publication. This is a cooperative effort between the FTC, the National Institute of Standards and Technology, the Department of Homeland Security and the Small Business Administration.

Guard against W-2 scams

All employers – in both the public and private sectors – also are targets for the W-2 scam that has in recent years become one of the more dangerous email scams for tax administration. These emails appear to be from an executive or organization leader to a payroll or human resources employee. It may start with a simple, “Hey, you in today?” and, by the end of the exchange, all of an organization’s Forms W-2 for their employees may be in the hands of cybercriminals. This puts workers at risk for tax-related identity theft.

Because payroll officials believe they are corresponding with an executive, it may take weeks for someone to realize a data theft has occurred. Generally, the criminals are trying to quickly take advantage of their theft, sometimes filing fraudulent tax returns within a day or two. This scam is such a threat to taxpayers that a special IRS reporting process has been established.

Here's an abbreviated list of how to report these schemes:

may be asked to file a report with their local law enforcement agency.
- Notify employees so they may take steps to protect themselves from identity theft. The Federal Trade Commission's www.identitytheft.gov provides guidance on general steps employees should take.
- Forward the scam email to phishing@irs.gov.

Employers are urged to put steps and protocols in place for the sharing of sensitive employee information such as Forms W-2. One example would be to have two people review any distribution of sensitive W-2 data or wire transfers. Another example would be to require a verbal confirmation before emailing W-2 data. Employers also are urged to educate their payroll or human resources departments about these scams.

The IRS, state tax agencies and the tax industry are committed to working together to fight against tax-related identity theft and to protect taxpayers. But the Security Summit needs help. People can take steps to protect themselves online.

Taxpayers can visit the "Taxes. Security. Together." awareness campaign or review IRS Publication 4524, Security Awareness for Taxpayers, for additional steps to protect themselves and their data from identity theft. Tax professionals can get more information through the Protect Your Clients; Protect Yourself campaign as well as the Tax Security 101 series.

Technology

(NASBA) as a sponsor of continuing professional education on the National Registry of CPE