IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

National Tax Security Awareness Week, Day 5: Security Summit partners remind businesses to tighten security; be aware of steps to help prevent, protect data loss

IR-2021-241, Dec. 3, 2021

WASHINGTON – The Internal Revenue Service, state tax agencies and the nation's tax industry urged businesses to be alert to cyberattacks aimed at gaining access to business data and customer information and be aware of steps to help them on tax-related issues related to identity theft.

The partners, operating cooperatively as the Security Summit to fight identity theft, marked the final day of National Tax Security Awareness Week with a warning to businesses to use the strongest measures possible to protect their data and systems.

"Businesses, just like individuals and tax pros, need to stay alert," said IRS Commissioner Chuck Rettig. "Thieves may steal enough information to file a business tax return or use other scams that involve the company or its employees."

More than 70% of cyberattacks are aimed at businesses with 100 or fewer employees. Con artists can target credit card or payment information, the business identity information or employee identity information.

Businesses are encouraged to follow best practices from the Federal Trade Commission including:

- Set security software to update automatically,
- Back up important files,
- Require strong passwords for all devices,
- Encrypt devices and
- Use multi-factor authentication.

More information is available at FTC's Cybersecurity for Small Businesses.

Businesses should especially be alert to any COVID-19 or tax-related phishing email scams that attempt to trick employees into opening embedded links or attachments. IRS related scams may be sent to phishing@irs.gov.

Starting late last year, the IRS began masking sensitive information from business tax transcripts, the summary of corporate tax returns, to help prevent thieves from obtaining identifiable information that would allow them to file fake business tax returns.

Only financial entries are fully visible. All other information has varying masking rules. For example, only the first four letters of each first and last name – of individuals and businesses – will display. Only the last four digits of the Employer Identification Number will be visible.

The IRS also has the Form 14039-B, Business Identity Theft Affidavit (.pdf), that will allow companies to proactively report possible identity theft to the IRS when, for example, an e-filed tax return is rejected.

Businesses should file the Form 14039-B if it receives a:

- Rejection notice for an electronically filed return because a return already is on file for that same period.
- Notice about a tax return that the entity didn't file.
- Notice about Forms W-2 filed with the Social Security Administration that the entity didn't file.
- Notice of a balance due that is not owed.

This form will enable the IRS to respond to the business much faster than in the past and work to resolve issues created by a fraudulent tax return. Businesses should not use the form if they experience a data breach but see no tax-related impact. For more information, see Identity Theft Central's Business section.

Although various tax scams can come and go, all employers should remain alert to Form W-2 theft schemes. In the most common version, a thief poses as a high-ranking company executive who emails payroll employees and asks for a list of employees and their W-2s. Businesses often don't know they've been scammed until an employee reports a fraudulent tax return has been filed.

There is a special reporting procedure for employers who experience the W-2 scam. It also may be found at Identity Theft Central's Business section.

Finally, Security Summit partners urge businesses to keep their EIN application information current. Changes of address or responsible party may be reported using Form 8822-B. Reminder: Changes in the responsible party must be reported to the IRS within 60 days. Current information can help the IRS find a point of contact to resolve identity theft and other issues.

The IRS, state tax agencies, the private sector tax industry, including tax professionals, work in partnership as the Security Summit to help protect taxpayers from identity theft and refund fraud. This is the final installment in a week-long series of tips to raise awareness about identity theft.

See IRS.gov/securitysummit for more details. Also, check out the most recent *A Closer Look* column on National Tax Security Awareness Week here.

-30-