Tax Related Identity Theft

Posted At : June 25, 2019 10:06 AM | Posted By : Admin
Related Categories: Security

April 15 has come and gone, but that doesn't mean the scammers have moved on.

Tax-related identity theft is prominent on the **IRS's 2019 Dirty Dozen list of Tax Scams**. Tax-related identity theft is not limited to stealing personal information of individuals. Because of successful efforts to crack down on such identity theft, thieves have shifted their focus to businesses. They create and use, or attempt to use, the identifying information of businesses to obtain tax benefits. For example, as the **IRS has noted**, cybercriminals that obtain a business's tax identification number may file a return claiming a tax refund because of a fuel credit or a research credit used as a Social Security tax offset.

Signs of identity theft

It's essential for you as a business owner to understand that tax-related identity theft is real and could hit your company. Vulnerability exists regardless of the size of a company (amount of revenues, value of assets, or number of employees). The IRS lists 5 signs of identity theft:

1. The IRS rejects an e-filed return saying it already has one with that employer identification number (EIN) or Social Security number (SSN).
2. The IRS rejects an extension to file request (Form 7004 for entities; Form 4868 for Schedule C or F filers) saying it already has a return with that EIN or SSN.
3. The business receives an unexpected tax transcript.
4. The business receives an IRS notice that doesn't relate to anything they submitted.
5. The business doesn't receive expected or routine mailings from the IRS.

Recognize and avoid identity theft schemes

Identity thieves are continually creating new scams to utilize business information to their financial advantage. Here are some examples of previous scams to look out for:

- **Form W-2/SSN data.** Cyber thieves use spoofing techniques to make an email appear as if it is from a company 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, referred to as business email compromise (BEC) or business email spoofing (BES), enables criminals to use employees' personal information to commit tax fraud and financial theft. If your business data is compromised, tell employees and alert the IRS at **dataloss@irs.gov**.
- **Direct deposit changes.** An email from cybercriminal posing as an employee asks the payroll or HR department to change his/her direct deposit of salary or wages. A new bank account is provided, which is used to siphon off an employee's compensation.

Big tipoffs that emails are from scammers are poor grammar and misspellings. The IRS has provided this example of a wire transfer scam: *"Please confirm the receipt of my message, Authorized can you handle domestic transfer payment now?"*

Steps for safeguarding tax information

Protection from tax-related identity theft should be part of your overall best practices for data protection from hackers and scammers.

- **Use basic security measures.** You can learn more from **Small Business Information**

Security: The Fundamentals

- **Work with good tax pros.** Be sure your CPA or other tax professional is safeguarding your tax information. A good tax pro can also help you identify cybersecurity weaknesses in your business. The AICPA offers members the opportunity to obtain a Cybersecurity Advisory Services Certificate*; those who obtain this designation are better trained to help business clients with their cybersecurity.
- **Learn more.** See IRS Publication 4557: Safeguarding Taxpayer Data: A Guide for Your Business.