MICHIGAN ATTORNEY GENERAL

CONSUMER ALERT

TAX SCAMS TARGETING SMALL AND MID-SIZED BUSINESSES

As small and mid-sized businesses (SMBs) become increasingly vulnerable to cybercrime, they have also become ideal targets for data thieves during tax season. Scammers have found that fraud tricks that work against individuals are successful against SMBs, too.

Watch out for these tactics and scams targeting SMBs year-round — but especially during tax season.

TAX SCAMS TARGETING BUSINESSES:

Business-Related W-2 Scams

W-2 scams occur when hackers use fake emails or text messages to lure payroll and human resources professionals to share sensitive tax information and gain access to employees' W-2 Forms. It is a threat to company data and employees.

The IRS reports that the messages may say something like "I am analyzing some reports and need a copy of your W-2's for last year. Please send ASAP." Once the W-2's are in the cybercriminals' hands, they file fake tax returns for refunds.

The IRS recommends that companies review their policies for sharing employee data and consider having two people review any request for W-2 data before approving its distribution.

Companies can also help prevent tax-related identity theft if they file their W-2 information with the IRS before the end-of-March deadline. Because tax refunds may be issued before employer W-2 information is received and verified by the IRS, fraudsters potentially have a two-month window between the end of January (when employers must give employees their W-2 forms) and the end of March (when employers must file that information with the IRS).

Employee Identification Number Scams

This scam occurs when companies applying for Employer Identification Numbers (EINs) are tricked into signing up through fraudulent websites. An EIN is required for business bank, loan and credit accounts as well as state and federal tax filing. Only apply for your EIN by filing an SS-4 Form through the IRS.

Red flags that indicate that your business identity has been stolen:

- Your electronically filed return is rejected because a return with your company's EIN is already on file.
- Your request for an extension is rejected because a return with your company's EIN is already on file.
- Your business receives an unexpected tax transcript receipt or IRS notice that doesn't correspond to your return.
- You fail to receive expected communication from the IRS because fraudsters have changed the address on your application.

The IRS is calling

The most frequently reported scam involves criminals who call and claim to be from the IRS and say you or your company owe taxes. Often the callers leave messages with a phone number to call back that never works or only works for a short period of time, making it hard for law enforcement to track them.

You know it is a scam because the caller will tell you that the matter is urgent, and if you want to avoid additional penalties or jail, you must pay immediately using a suspicious payment form like a pre-paid debit card, a wire transfer, an iTunes card or other method that is difficult for law enforcement to trace. The caller ID might show it's the IRS and the caller might even provide a real IRS agent's name and badge number. In reality, the caller ID is faked, and the caller is a criminal intent on stealing your money.

If you owe the IRS money, the IRS will first contact you by mail — and they will never ask you to pay with a suspicious payment form. Acceptable IRS full payment forms include electronic fund transfers using your back account; checks, money orders, debit or credit card payments via phone or internet, and cash payments made in person with an IRS retail partner. More payment details, including installment agreement information is available on the IRS webpage.

Fake IRS calls are so prevalent that the federal government has a specific IRS Impersonation Scam Reporting website.

KNOW THIS: The IRS does not call, text or email you and demand immediate payment. Anybody contacting you claiming to be from the IRS and asking you for personal or financial information is a crook.

Excessive claims for business credits

This is not your typical scammer-commits-fraud-and-steals-from-victim type scam, but it does appear on the IRS' list of "Dirty Dozen" Scams. The IRS warns SMBs to beware of unscrupulous tax preparers who encourage businesses to claim tax credits to which they are not entitled.

Two credits often targeted for abuse and on the IRS' radar are the Research Credit and the Fuel Tax Credit. Each of these credits has specific eligibility criteria and the IRS warns SMBs to watch out for suggestions to make improper claims on their tax returns. Falsely claiming these credits subjects both the taxpayer and preparer to penalties. Read the IRS release about how to avoid making these improper claims.

The IRS urges you to confirm your tax preparer's credibility by asking for their Preparer Tax Identification Number and to not trust your business information to anyone without first verifying their Certified Public Accountant (CPA) status. To verify your CPA's license in Michigan, use the Department of Licensing and Regulatory Affairs' online search engine.

PROTECT YOUR SMALL BUSINESS FROM TAX SCAMS

The Attorney General recommends SMBs create a system of checks and balances and:

- Have a trusted member of your executive team or an independent tax agent double check your processes.
- Train employees to recognize W-2 phishing scams.
- Beware of IRS impersonators.
- Remember: the IRS will never call or email you for tax-related information. They will first contact your organization through the mail.

COMMON SCAM TACTICS:

Phishing and Vishing

Phishing schemes involve scammers sending text or email messages to trick you into giving them personal information or access to sensitive files. Vishing (voice phishing) is just like phishing, but it uses the phone to commit the fraud. These messages look like they are from a company or entity you know and trust. They often tell a story to trick you into clicking a link or opening an attachment. Watch for messages that may say:

- We've noticed some suspicious activity or log-in attempts;
- There's a problem with your account or your payment information;

- We need you to confirm some information;
- We need an invoice paid by close of business today; or
- Here's a link you can click to make a payment.

Don't take the bait. If you or one of your employees gets a suspicious email, text message or phone call and you do not have an account with the company or know the person who contacted you, assume you are being scammed and delete the message or hang up. If you do have an account with the company, then contact it using a website or phone number you use and know to be accurate.

Government Imposter

Contact from the government gets your attention. Criminals use real government references and the threat of government action to trick you into taking action that will help them steal from you. The initial contact could come in any form—letter, phone call, email, or text message. No matter the form, the goal is the same: to get your personal or business information and steal your money.

If you get a text or email from someone claiming to be from a government agency with an attachment or link asking you to open it or click on it, do not do it until you verify it is authentic. The attachment or link might contain malware. If you click to open the attached file (typically, a zip file) in a government imposter scam, you will open a virus or other malware and infect your computer or mobile device and allow criminals to steal your company's information, monitor your online activity, and commit fraud.

Scammers know that the threat of government action will cause many recipients to open the attachment out of curiosity or concern. Always be very cautious of any unsolicited email or text.

KNOW WHO TO CONTACT

- Contact the Treasury Inspector General for Tax Administration to report a phone scam. Use their "IRS Impersonation Scam Reporting" web page. You can also call 800-366-4484.
- Report phone scams to the Federal Trade Commission. Use the "FTC Complaint Assistant" on FTC.gov. Please add "IRS Telephone Scam" in the notes.
- Report to the IRS at phishing@irs.gov an unsolicited email claiming to be from the IRS, or an IRS-related component like the Electronic Federal Tax Payment System.
- Businesses that discover an email compromise should also report it to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3).

CONTACT THE ATTORNEY GENERAL'S OFFICE

If you have a general consumer complaint, you may file a complaint with the Attorney General's Consumer Protection Unit:

Consumer Protection Unit
P.O. Box 30213
Lansing, MI 48909
517-335-7599
Fax: 517-241-3771
Toll free: 877-765-8388
Online complaint form