SMB ALERT
BEWARE OF 2019 TAX SCAMS

The National Cyber Security Alliance’s Advice and “Take Action” Tips

Whether a family-owned restaurant, a healthcare service provider in a rural market or a local real estate office, companies of all sizes and industries are gearing up for tax filing season. Tax time is a haven for hackers as many small to medium-sized businesses (SMBs) are not properly prepared to combat data scams. With the unprecedented growth in conducting commerce online, SMBs face the ongoing risk of cyberattacks.

According to a very timely summary provided by Fighting Identity Crimes, two of the most popular scams in 2019 target W-2s and tax preparers.

W-2 Scams

- The Internal Revenue Service (IRS) recently warned SMBs of the rapidly growing threat of W-2 scams. Using phony emails, hackers lure payroll and human resources personnel to hand over sensitive tax information, potentially letting your employees’ W-2 forms fall into hackers’ hands.
- In another unscrupulous scheme, companies applying for Employer Identification Numbers (EINs) are being duped into signing up via fake websites. Similar to a Social Security number, your EIN is required for loans and credit accounts in addition to state and federal tax filing. Apply for your EIN by filing a SS-4 Form only through the IRS.
Targeting Tax Preparers

- **Tax preparers** are often SMBs themselves, serving local communities and regional businesses. Their files are filled with tons of tax information and highly sensitive client data. In 2018, the IRS received *five to seven reports per week* from tax professionals who experienced data theft.
- Tax preparers are required by the IRS to generate and implement a *security plan* to protect client data along with their computer networks from a potential hack. A good rule of thumb is to check your tax preparer’s credibility by requesting their *Preparer Tax Identification Number*. It is also smart to verify their CPA status.

The National Cyber Security Alliance (NCSA) has invaluable tips and advice for SMBs of varying industries. Taking simple, actionable steps can go a long way in helping to protect the company’s data along with the personal information of your employees and customers during a period of high online traffic.

**Keep All Machines Clean**
Whether you are a professional tax preparer filing your own personal or business taxes, having updated software on all devices that connect to the internet is critical. This includes security software, web browsers and operating systems for PCs and your mobile devices. Don’t forget about devices employees use at home or on the road as well. Having current software is a strong defense against viruses and malware that can steal login credentials or use your computer to generate spam.

**Do a Deep Data Dive**
Preparing for tax season is a great time to identify and document what data you create, collect, store, transmit, etc. Determine what information you handle or store out of business necessity and safely dispose of any unnecessary data. Keep in mind that this goes for paper documents, too. Also, consider *encrypting* data both in transit and at rest to protect it from cybercriminals. The Center for Internet Security shares tips for information disposal.

**Get Savvy About Wi-Fi Hotspots**
Do your employees work remotely? What about staff travel? These are realities of running a business. It is critical to keep in mind that wherever you are conducting business, public wireless networks are not secure. Cybercriminals can potentially intercept internet connections while you are filing highly personal information via public WiFi. Make it a rule for employees to access your business data from a secure network and establish clear expectations through policies and procedures for how and on what devices your team can access your network. Check out the U.S. Department of Homeland Security’s Cybersecurity While Traveling Tip Card.
SMB ALERT
BEWARE OF 2019 TAX SCAMS

When in Doubt, Throw It Out
Malicious emails are often the point of entry for cybercriminals to gain access to your business information. Tax season is prime time for scammers to ramp up their efforts. If an email looks suspicious -- even if you know the source -- it’s best to delete. Or, verify the legitimacy of the email via a different method of communication like a quick phone call or text. Train all employees on what to look for in a suspicious email – ideally, prior to providing them access to email. Need help? MediaPRO has a “How to Spot a Phishy Email” infographic in this Cybersecurity Awareness Toolkit and Google recently released a free Phishing Quiz.

Lock Down Your Login
Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Be sure employees are not sharing passwords with each other. In addition, lock down access to sensitive data so that only those who need it can retrieve it.

Make Better Passphrases
If your passphrases are too short or easy to guess, it’s like giving a cyber thief your banking PIN. Longer passwords and those that combine capital and lowercase letters with numbers and symbols provide better protection. Place a strong emphasis on helping employees understand the makings of strong passphrases and why they are so important to keeping the company safe and secure. The National Institute of Standards and Technology (NIST) shares user-friendly guidance on creating strong passphrases.

Have a Plan in Place
Know how to respond if you are the victim of a security breach. Who do you turn to for assistance? What’s your state’s data breach notification law? Does your insurance cover losses from a cybercrime? Create and practice your response plan before you have an incident. The Federal Trade Commission’s Data Breach Response Guide and Department of Justice’s Best Practices for Victim Response and Reporting of Cyber Incidents guide will help you identify some response strategies.

CyberSecure My Business™ Monthly Webinars and Regional Events
In October 2017, NCSA launched CyberSecure My Business™. The program – of which FedEx is a Founding Partner, Trend Micro is a Signature Sponsor and InfoSec Institute is a Contributing Sponsor – was created to help protect the cybersecurity in the small and medium-sized business (SMB) community. It does so by offering interactive training based on the NIST Cybersecurity Framework. Join NCSA for monthly webinars and in-person events in regional markets.