NATIONAL CYBER SECURITY ALLIANCE

Tax Season Cybersecurity for Small Business

Moderated by
Daniel Eliot, Director
Small Business Programs
National Cyber Security Alliance

Charles A Harwood, Director
Northwest Region
Federal Trade Commission

Jerry Sparkman, Director
Information Technology
National Association of Tax Professionals
Goal of 5-Step Approach Is Resilience

Know the threats and **Identify** and **Protect** your assets

**Detect** problems and **respond** quickly and appropriately

Know what **recovery** looks like and prepare

---

Thanks to our National Sponsors

[Logo of Trend Micro]

[Logo of Initiative for Education]

[Logo of InfoSec Institute]
San Jose CyberSecure My Business™ Workshop

When:  March 25, 2019
       9am-12pm

To Register:  https://cybersecuremybizsanjose.eventbrite.com

Where:  Silicon Valley United States
         Patent and Trademark Office
         26 South Fourth Street
         San Jose, CA 95113

Presented By:
National Signature Sponsor
National Contributing Sponsor
Local Event Sponsor:
Securing Sensitive Tax Information

Federal Trade Commission
Presentation Overview

- Tax identity theft
- Data security
- Assisting tax identity theft victims

Filing a fraudulent tax return using another person’s Social Security Number

Working and not paying taxes using another person’s Social Security Number
Trends

- Tax identity theft can affect anyone regardless of age, gender, race or socio-economic status

- Tax identity theft is one of the top forms of identity theft reported to the FTC
  - Complaints about traditional tax identity theft are down since 2017
  - Complaints about employment-related identity theft are up since 2017

- 10 times as many Social Security imposter scam reports in 2018
How Does Tax Identity Theft Happen?

- Imposters
- Data breaches
- Malware
- Phishing/spear phishing
Steps Consumers Can Take to Reduce Risk

- Safeguard confidential information
- Share personal information carefully
- Monitor statements and credit reports
- Dispose of personal information safely
- Follow good filing practices
IdentityTheft.gov can help you report and recover from identity theft.

**HERE'S HOW IT WORKS:**

1. **Tell us what happened.**
   - We’ll ask some questions about your situation. Tell us as much as you can.

2. **Get a recovery plan.**
   - We’ll use that info to create a personal recovery plan.

3. **Put your plan into action.**
   - If you create an account, we’ll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.
Which statement best describes your situation?

- I want to report identity theft.
- Someone else filed a Federal Tax return using my information.
- Someone has my information or tried to use it, and I'm worried about identity theft.
- My information was exposed in a data breach.
- Something else.
IdentityTheft.gov

Report Identity Theft to the FTC and the IRS

Next, we are going to ask for specific details. We will use the information you provide to create your:

- FTC Identity Theft Report
- IRS Identity Theft Affidavit
- Recovery Plan

These will help you fix problems caused by the identity theft.
Great. Your account has been created!

Here, you can download your FTC Identity Theft Report, or interact with your recovery plan.

Click on the first step, and we’ll guide you through the process. We’ve pre-filled letters and forms to make it easier for you.

You have successfully submitted your IRS Identity Theft Affidavit (Form 14039).

Please complete the remaining recovery plan steps.

Your Recovery Plan

- Contact the IRS.
- Place a fraud alert on your credit reports.
- Review your credit reports for fraud.
- Consider placing an extended fraud alert or credit freeze.
- Report identity theft to the FTC.
Start with Security

Lead by example to create a culture of security at work

- Factor security into data-related decisions
  - What kinds of information do you collect?
  - How long do you keep it?
  - Who do you share it with?
  - Who has access?
Two Plans

- IT Security Plan
  - Physical Security
  - Electronic Security
  - Educate Employees
- Data Breach Response Plan
Ftc.gov/cybersecurity

- Cybersecurity Basics
- NIST Cybersecurity Framework
- Physical Security
- Ransomware
- Phishing
- Business Email Imposters
- Tech Support Scams
- Vendor Security
- Cyber Insurance
- Email Authentication
- Hiring a Web Host
- Secure Remote Access
Cybersecurity Basics

PROTECT YOUR FILES & DEVICES

Update your software
This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files
Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords
Use passwords for all laptops, tablets, and smartphones. Don’t leave these devices unattended in public places.

Encrypt devices
Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication
Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that’s inserted into a computer.
NIST Cybersecurity Framework

1. IDENTIFY
Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:
- Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.
- Steps to take to protect against an attack and limit the damage if one occurs.

2. PROTECT
- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

3. DETECT
- Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.
- Investigate any unusual activities on your network or by your staff.
- Check your network for unauthorized users or connections.
Secure Remote Access

Employees and vendors may need to connect to your network remotely. Put your network's security first. Make sure employees and vendors follow strong security standards before they connect to your network. Give them the tools to make security part of their work routines.

How to Protect Devices

Whether employees or vendors use company-issued devices or their own when connecting remotely to your network, those devices should be secure. Follow these tips—and make sure your employees and vendors do as well:

- Always change any pre-set router passwords and the default name of your router. And keep the router's software up to date; you may have to visit the router website often to do so.
- Consider enabling full-disk encryption for laptops and other mobile devices that connect remotely to your network. Check your operating system for this option, which will protect any data stored on the device if it's lost or stolen. This is especially important if the device stores any sensitive personal information.
- Change the employees' settings to stop automatic connections to public Wi-Fi.
- Keep up-to-date antivirus software on devices that connect to your network, including mobile devices.

What to Do to Maintain Security

Train your staff:

- Include information on secure remote access in regular trainings and new staff orientations.
- Have policies covering basic cybersecurity. Give copies to your employees, and explain the importance of following them.
- Before setting any device — whether at an employee's home or a vendor's network — connect to your network, make sure it meets your network's security requirements.
- Tell your staff about the risks of public Wi-Fi.

Give your staff tools that will help maintain security:

- Require employees to use unique, complex network passwords and avoid unattended, open workstations.
- Consider creating a VPN for employees to use when connecting remotely to the business network.
- Require multi-factor authentication to access areas of your network that have sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's registered into a computer.
- If you offer Wi-Fi on your business premises for guests and customers, make sure it's separate from and not connected to your business network.

Learn More at: FTC.gov/SmallBusiness
Business Email Imposters

How to Protect Your Business

- **Use email authentication**
  When you set up your business’s email, make sure the email provider offers email authentication technology. That way, when you send an email from your company’s server, the receiving servers can confirm that the email is really from you. If it’s not, the receiving servers may block the email and foil a business email imposter.

- **Keep your security up to date**
  Always install the latest patches and updates. Set them to update automatically on your network. Look for additional means of protection, like intrusion prevention software, which checks your network for suspicious activity and sends you alerts if it finds any.

- **Train your staff**
  Teach them how to avoid phishing scams and show them some of the common ways attackers can infect computers and devices with malware. Include tips for spotting and protecting against cyber threats in your regular employee trainings and communications.
WHAT SHOULD YOUR CYBER INSURANCE POLICY COVER?

Make sure your policy includes coverage for:

- Data breaches (like incidents involving theft of personal information)
- Cyber attacks on your data held by vendors and other third parties
- Terrorist acts
- Cyber attacks (like breaches of your network)
- Cyber attacks that occur anywhere in the world (not only in the United States)

Also, consider whether your cyber insurance provider will:

- Defend you in a lawsuit or regulatory investigation (look for “duty to defend” wording)
- Provide coverage in excess of any other applicable insurance you have
- Offer a breach hotline that’s available every day of the year at all times

The FTC thanks the National Association of Insurance Commissioners (NAIC) for its role in developing this content.
Data Breach Response Plan

- Notify law enforcement and legal team
- Secure operations
  - Assemble your team
  - Secure physical area
  - Stop additional losses
- Fix vulnerabilities
  - Alert service providers and others
  - Forensic analysis
- Recover
Cybersecurity and Your Small Business
Topic: Online Safety & Security
Language: English
Format: Booklet

Information on 12 different cybersecurity topics to help small business owners and staff understand common cyber threats and how they can protect their business.

Data Breach Response: A Guide for Business
Topic: Privacy & Identity
Language: English
Format: Booklet

Practical steps for businesses when responding to a data breach.

Topic: Online Safety & Security
Language: English
Format: Booklet

What can companies learn from the FTC’s 50+ data security cases?
Lesson #1: Start with security.
NATIONAL CYBER SECURITY ALLIANCE
Tax Season Cybersecurity for Small Business

Jerry Sparkman, Director
Information Technology

NATP
National Association of Tax Professionals
Protecting Tax Identity and Navigating a Relationship with a Tax Professional
Jerry Sparkman

Information Technology Director for the National Association of Tax Professionals

20 Years Experience in Technology Industry

Battles internet ‘Evil Doers’

Helps Safeguard Tax Professionals
NATP is the largest association dedicated to equipping tax professionals with the resources, connections and education they need to provide the highest level of service to their clients. NATP is comprised of over 22,000 leading tax professionals who believe in a superior standard of ethics and exemplify professional excellence.
Tax Identity Protection

• Why would someone want your tax identity?
• Tax pro tips to protect identity
• Working with a tax pro
• Tips from Jerry to protect your identity
Why Would Someone Want Your Tax Identity?

- Scammers file a false tax return using your identity
- Scammers route the refund to an address or bank account
- Only need SSN or EIN and Name
- IRS accepts only first return
- Subsequent filings will not process
- Other forms of identity theft
Top 5 Identity Fraud Protection Tips From Tax Pros

- **Moving**
  - File form 8822 change of address
- **IRS never initiates contact via email**
  - Usually only USPS, sometimes call
- **Guard W-2’s**
  - Beware of anyone asking for W-2 information for you or your staff
- **Identity compromised?**
  - File form 14039 to get a security pin that is required to file
- **File early**
Tax Pros Are Well Aware

- Tax pro social engineering attacks have been on the rise since 2017
  - Phishing
  - Vishing
- On average, a tax firm will have 300 returns on file
  - That’s 300 “tax identities”
To: undisclosed-recipients:
Subject: Tax Refund

Good morning,

We are couple requiring a few question on filing our 2017 Tax refunds with you:-

Please can you kindly give us more information on filing our 2017 tax refunds such as what type of form do we require and do we have to provide our SSN, Drivers License? Can we file Children together? We have our Form 1040 Ready and will furnish you upon hearing from you and how much does it cost to assist us with the filing?

Thanks
Charles Anderson

Send tax phishing emails to:
Phishing@irs.gov
Phishing@natptax.com
From: William
To: [email]
Subject: Our 2016 Taxes

Hello Joseph,

Are you still accepting new clients, as we need to file our 2016 Taxes

Regards,
William M & Christina A Hickey

From: James
Date: March 27, 2017 8:06:59 AM CDT
Reply-To: Good afternoon,

I am in search of a tax preparer who would help me review, prepare and file my Business and personal return for 2016. I already have my W-2 form. Please let me know the possibility and possibly an estimated cost.

Thanks for your prompt reply.

Regards,

From: Kenneth Hoyle
Sent: Thursday, February 9, 2017 9:32 AM
To: "For Preparer"
Subject: Tax Preparation

I need a Tax Preparer to help with my return, let me know if you are available. Kindly get back to me via my email.

Regards,
Ken.

From: William Macheski, M.D., F.A.C.C.
President/CEO
Columbus Cardiology Associates

Hi
I found you on IRS website that you are a tax preparer around me. Please let me know what you will be needing.
Thanks

From: Alex
Sent: Thursday, January 26, 2017 6:04 AM
Subject: Taxes 2016

Hi my name is Alex, i am presently out of the country on a job contract and would be able to file my taxes for 2016? what informations do you need and how much will it cost me? your response is highly appreciated.

Regards
Alex
Establishing a Relationship with a Tax Pro

- May seem distrustful of your request
- Might require confirmation of your identity
  - Meet in person
  - Call back number
  - Drivers license
  - Social security card
- You should also seek validation of identity from the tax pro
  - Did they contact you or did you contact them?
Safely Communicating with a Tax Pro

- Portals
  - Use file sharing service provided by Tax Pro
- Encrypt documents
  - Password protect documents
- Call ahead
  - Let them know files are coming
Tips From Jerry

- Be wary of anyone requesting SSN or EIN or W-2
- Verify communications via a secondary channel
  - Call/text
- Use multi factor authentication
  - 2 Step Verification
- Keep companies where you disclose personal information to a minimum
- Follow information security best practices
  - FTC guidelines on cybersecurity
- Spread the word about tax identity fraud
  - Attend and sponsor training
Thank you for your interest in this important topic.

To find a qualified tax professional, look to an NATP member.

taxprofessionals.com/natp-members
Webinar Series
Second Tuesdays
2:00 p.m. EST

Up-Coming Webinars:
• March 19th  Cyber threats to precision agriculture

• April 9th   Time for a “Digital Spring Cleaning”

To Register: www.staysafeonline.org
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.

Apply the following tips when communicating online or answering calls:

1. Verify the sender.
2. Do not disclose sensitive information.
3. Don't fall for fake websites.
4. Use strong passwords.
5. Protect your credit accounts in addition to state and federal tax filing. Apply the same vigilance to online and mobile banking accounts.

NATIONAL CYBER SECURITY ALLIANCE
Tax Season Cybersecurity for Small Business

Founding Sponsor
FedEx
smallbusiness.fedex.com

Signature Sponsor
Trend Micro
www.trendmicro.com

Contributing Sponsor
Infosec Institute
www.infosecinstitute.com

National Association of Tax Professionals
www.natptax.com

National Cyber Security Alliance
www.staysafeonline.org/cybersecure-business

Federal Trade Commission
www.FTC.gov/smallbusiness