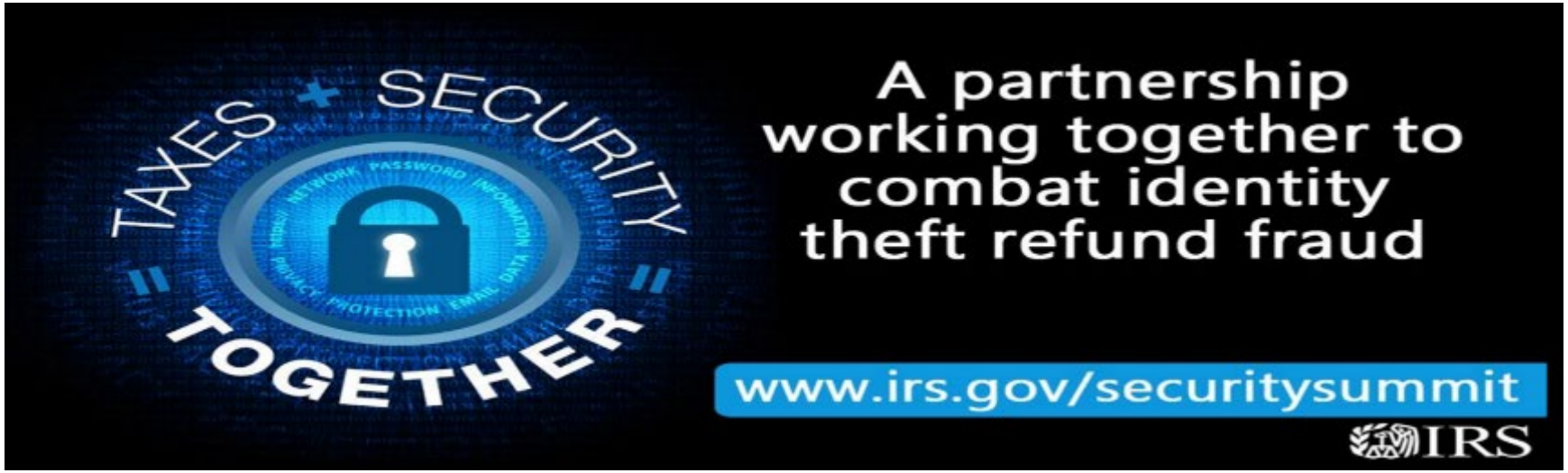
Scams and Tax Related Identity Theft
For Individuals and Businesses

Len Steinberg, EA
Robert Glantz, CID
Glenn Gizzi, IRS

Security Summit

The IRS, state tax agencies, and the tax community are working in partnership to combat identity theft refund fraud to protect the nation's taxpayers.



Common Scams

- Email, Phishing and Malware Schemes
- Fake Charities
- Threatening Impersonator Phone Calls
- Refund Theft
- Scams targeting non-English speakers
- Unscrupulous Return Preparers
- Employee Retention Tax Credit

Spotting Phishing Emails

- The email asks you to confirm personal information
- The web and email addresses do not look genuine
- It’s poorly written
- There’s a suspicious attachment
- The message is designed to make you panic

Preventing Online Identity Theft

Don’t respond to suspicious IRS emails, Texts and Faxes

Secure your computers (i.e., firewalls, anti-virus/anti-phishing/anti-spam, etc.)

Use strong passwords

Back up critical personal information

Limit the personal information you provide on social media

Visit OnGuardOnline.gov - IRS.gov/IDTheft – StaySafeOnline.org

Know the Signs of Tax-Related Identity Theft

- **E-Filed return rejects due to duplicate Social Security Number.**

Form **14039** (March 2022)	Department of the Treasury - Internal Revenue Service **Identity Theft Affidavit**	OMB Number 1545-2139

This affidavit is for **victims** of identity theft. To avoid delays do not use this form if you have already filed a Form 14039 for this incident.
The IRS process for assisting victims selecting **Section B**, **Box 1** below is explained at irs.gov/victimassistance.
Get an IP PIN: We encourage everyone to opt-in to the Identity Protection Personal Identification Number (IP PIN) program. If you don't have an IP PIN, you can get one by going to irs.gov/ippin. If unable to do so online, you may schedule an appointment at your closest Taxpayer Assistance Center by calling (844-545-5640). Or, if eligible, you may use IRS Form 15227 to apply for an IP PIN by mail or FAX, also available by going to irs.gov/ippin.

Section A - Check the following boxes in this section that apply to the specific situation you are reporting *(required for all filers)*

1. I am submitting this Form 14039 for myself
2. I am submitting this Form 14039 in response to an IRS Notice or Letter received
   - Provide 'Notice' or 'Letter' number(s) on the **line to the right** _____
   - Check box 1 in **Section B** and see special mailing and faxing instructions on reverse side of this form.
3. I am submitting this Form 14039 on behalf of my dependent child or dependent relative
   - Complete **Sections A-F** of this form. Do not use this form If dependent's identity was misused by a parent or guardian in filing taxes, this is not identity theft.
4. I am submitting this Form 14039 on behalf of another person living or deceased *(other than my dependent child or dependent relative)*
   - Complete **Sections A- F** of this form.

- **Letter from the IRS inquiring about a suspicious tax return that you did not file.**

Know the Signs of Tax-Related Identity Theft – continued (cont.)

- You get an IRS notice that you owe additional tax or refund offset, or that you have had collection actions taken against you for a year you did not file a tax return.

- You receive a Form W-2 or Form 1099 from an employer for whom you didn't work or benefits from a government agency, or IRS records indicate you received wages or other income from an employer you didn't work for.

Reporting Scams and Theft

- Unsolicited emails or social media attempts to gather information that appear to be from either the IRS or an organization closely linked to the IRS, should forward the message to phishing@irs.gov.
- www.IdentityTheft.gov – One-stop Resource
- Scams, fraud, refund or Economic Impact Payment theft - Treasury Inspector General for Tax Administration (TIGTA). Reports can be made online at TIPS.TIGTA.GOV.

The Identity Protection PIN (IP PIN)

Proactively protect your federal tax account from identity theft.

What is the IP PIN?

- An Identity Protection PIN (IP PIN), is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number
- Even though you may not have a filing requirement, an **IP PIN still protects your account from fraudulent filings**
- An electronically filed return filed without your IP PIN, or an incorrect IP PIN, will reject, including your return and any fraudulent returns using your Social Security Number.
- Any paper returns filed without your correct IP PIN will undergo additional scrutiny and any fraudulent returns will be removed from your account. If the return verifies to be yours, we will continue to process it.

IRS IP PIN Opt-in Program

- As of January 2021, all taxpayers who can verify their identities may obtain an IP PIN to protect their tax returns
- One-time registration process
- Use online tool each January to obtain your IP PIN
- Review the process at www.IRS.gov/IPPIN

Important Reminders

- IP PIN protects your federal tax account from Identity Theft
- An IP PIN is valid for one calendar year, each year a new IP PIN is generated for your account
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns
- **Never share your IP PIN with anyone** other than your tax preparer at the time of filing
- If unable to enroll online there are alternatives
  - Form 15227, Application for an IP PIN
  - In-Person Meeting at a local Taxpayer Assistance Office, (TAC)
- IP PIN participants must keep their address current including dependents
  - By filing Form 8822, Change of Address

Do not share IP PIN

Do not share your IP PIN with anyone but your trusted tax provider

If you do your own taxes, enter IP PIN when asked by the software product

No one will call, email or text you to request your IP PIN

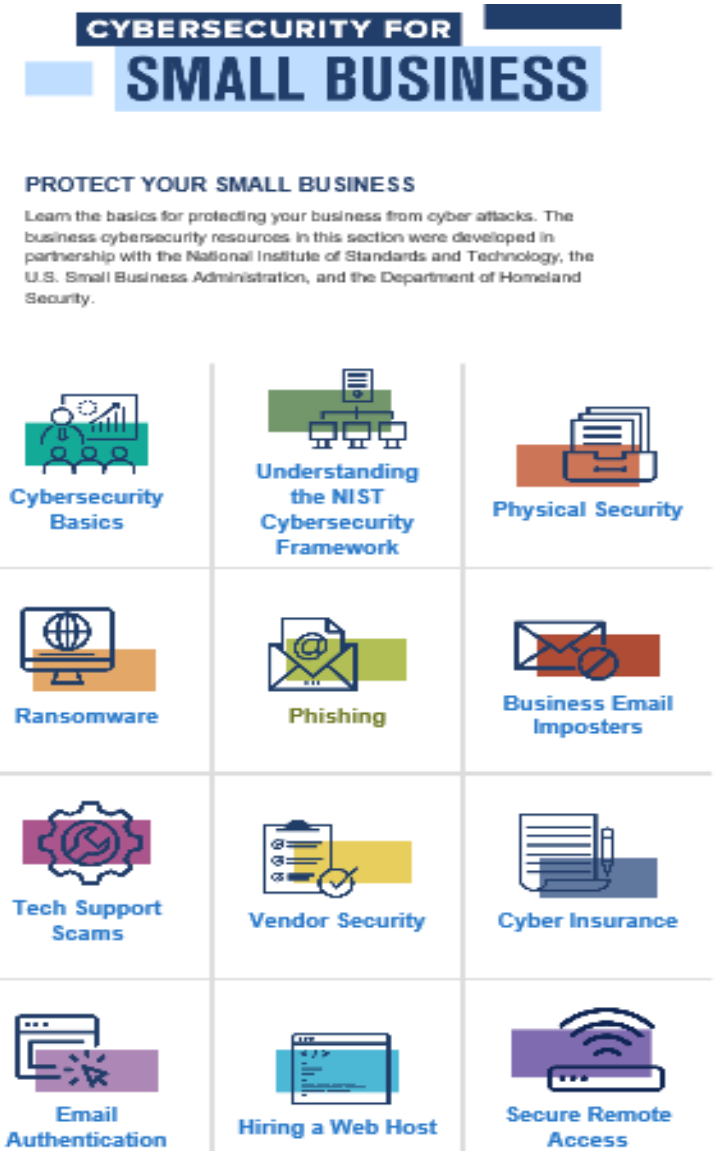
Quick Security Tips from the IRS:

Businesses at risk for Identity Theft

Small businesses are at risk

- 70% of cyberattacks on businesses with 100 or fewer employees
- Review and implement recommendations from the Federal Trade Commission
- “Cybersecurity for Small Business” at www.FTC.gov

Cybersecurity for Small Business



Cybersecurity basics to protect your files

- Protect your files
- Keep your security software updated
- Secure important files
- Require strong passwords for all devices
- Encrypt devices.
- Use multi-factor authentication

Protect Your Wireless Network

- Secure your router
- Use at least WPA2 encryption

Phishing Scams

- Phishing email or text
- Urgent message
- Link in email or text, or attachment to email
- May take you to a site that looks familiar, but it's part of the scam

Businesses may become victims of tax-related ID Theft

- COVID-19 scams
- Phishing email scams
- Fraudsters may file a false business tax return or false employment tax return

Steps to protect businesses

Masked business tax transcripts

- Financial entries visible
- Other information will be masked

W-2 Scam

- Thief poses as high-ranking company executive
- Thief asks for list of employees and W-2s
- Special reporting procedure at “Identity Theft Central” Business section.

Form 14039-B, Business Identity Theft Affidavit

File Form 14039-B if:

- Reject for an e-filed return that has already been filed
- Notice about tax return the entity didn't file
- Notice about W-2s the entity didn't file
- Notice of a balance due that is not owed

See more at "Identity Theft Central" Business section.

Businesses: keep your EIN information current

- Use Form 8822-B to report a change of address or a change in the responsible party.
- Current information can help the IRS find a point of contact to resolve identity theft issues.

Identity Theft Central

An official website of the United States Government

IRS

Help | News | English | Charities & Nonprofits | Tax Pros

File | Pay | Refunds | Credits & Deductions | Forms & Instructions | Search

Home / File / Individuals / Identity Theft Central

Identity Theft Central

English | Español | 中文 (繁體) | 한국어 | Русский | Tiếng Việt | Kreyòl ayisyen

- **Individuals**
  - How to File
  - When to File
  - Where to File
  - Your Information
  - Students
  - Employees
  - Parents
  - Military
  - Seniors & Retirees
- **Businesses and Self-Employed**
- **Charities and Nonprofits**
- **International Taxpayers**
- **Government Entities**

Tax-related identity theft happens when someone steals your personal information to commit tax fraud. Your taxes can be affected if your Social Security number is used to file a fraudulent return or to claim a refund or credit.

Information for Individuals

Taxpayer Guide to Identity Theft

Know the signs of identity theft, take action if you are a victim and protect your data and identity.

Taxes. Security. Together.

We all have a role to play in protecting your data.

Information for

Tax Professionals | Businesses

How We Combat Identity Theft

Security Summit
The IRS, state tax agencies and private industry partner to detect, prevent and deter tax-related identity theft and fraud.

Phishing and Online Scams
The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information.

IRS Commissioner Urges Taxpayers to Protect Their Data

Avoid Phishing Emails

Easy Steps to Protect

Remember, the IRS will never…

- Contact you by email, text or social media to ask for personal or financial data.
- Call to demand immediate payment using a prepaid debit card, gift card or wire transfer.
- Threaten to bring in police, immigration or other agencies to have you arrested.
- Ask for credit/debit card or other financial account information over the phone.
- Request login credentials, Social Security Numbers or other sensitive information.

Questions

Thank You!