Scams, Tax Related Identity Theft and Identity Protection PIN

Evelyn.Dyson.Lee@irs.gov
Sr. Stakeholder Liaison

Identity Theft Central
www.IRS.gov/IdentityTheft


STOP

Common Scams

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

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

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.

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

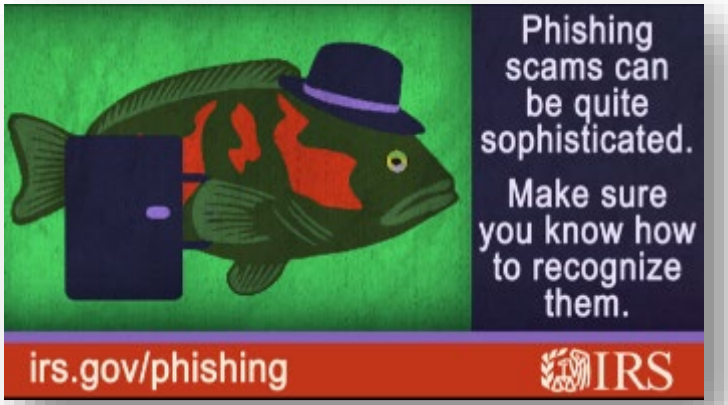
Know the Signs of Tax-Related Identity Theft

- e-Filed return rejects due to duplicate Social Security Number.
- Letter from the IRS inquiring about a suspicious tax return that you did not file.
- 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 income from an employer you didn't work for.

Reporting Scams and Theft – cont.

- 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



Pub 4524 Security Awareness

Security Awareness For Taxpayers

TAXES. SECURITY. TOGETHER.

The IRS, the states and the tax industry are committed to protecting you from identity theft. We've strengthened our partnership to fight the nation's common enemy – the criminals – and to devote ourselves to a common goal – serving you. Working together, we've made many changes to combat identity theft. We are making progress. However, cybercriminals are constantly evolving, and so must we. The IRS is working hand-in-hand with your state revenue officials, your tax software provider and your tax professional. But, we need your help. We need you to join with us. By taking a few simple steps to protect all of your digital devices, you can better protect your personal and financial data online and at home.

Please consider these steps to protect yourself from identity thieves:

Keep Your Computer and Mobile Phone Secure

- Use security software and make sure it updates automatically; essential tools include:
  - Firewall
  - Virus/malware protection
  - File encryption for sensitive data
- Treat your personal information like cash, don't leave it lying around
- Use strong, unique passwords; consider a password manager
- Use 2-Factor Authentication
- Give personal information only over encrypted websites - look for "https" addresses
- Back up your files

Avoid Phishing Scams and Malware

Identity thieves use phishing emails to trick users into giving up passwords and other information. Don't take the bait. Look for:

- Emails that pose as trusted source, i.e. bank, tax provider;
- Emails with an urgent message, i.e. update your account now!, with instructions to open a link or attachment
- Never download software or apps from pop-up advertising
- Talk to family about online security, both with computers and mobile devices

Protect Personal Information

Don't routinely carry your or any dependents' Social Security card or documents with an SSN. Do not overshare personal information on social media. Information about past addresses, a new car, a new home and even your children help identity thieves pose as you. Keep old tax returns and tax records under lock and key or encrypted if electronic. Shred tax documents before trashing.

Avoid IRS Impersonators. The IRS will not call you with threats of jail or lawsuits. The IRS will not send you an unsolicited email suggesting you have a refund or that you need to update your account. The IRS will not request any sensitive information online. These are all scams, and they are persistent. Don't fall for them. Forward IRS-related scam emails to phishing@irs.gov. Report IRS-impersonation telephone calls at www.tigta.gov.

Additional steps:

- Check your credit report annually; check your bank and credit card statements often.
- Review your Social Security Administration records annually: Sign up for My Social Security at www.ssa.gov.
- If you are an identity theft victim and your tax account is affected, review www.irs.gov/identitytheft for details.

Pub 5027 ID Theft Info for Taxpayers

Identity Theft Information for Taxpayers

Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

You may be unaware that this has happened until you e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying it has identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS about:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages or other income from an employer for whom you did not work.

Steps for victims of identity theft

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at identitytheft.gov.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
  - www.Equifax.com 1-800-525-6285
  - www.Experian.com 1-888-397-3742
  - www.TransUnion.com 1-800-680-7289
- Close any financial or credit accounts opened by identity thieves

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided.
- Complete IRS Form 14039, *Identity Theft Affidavit*, if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach form to your paper return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

More information is available at: IRS.gov/identitytheft or FTC's identitytheft.gov.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, *Identity Theft Affidavit*, only if your Social Security number has been compromised and IRS has informed you that you may be a victim of tax-related identity theft or your e-file return was rejected as a duplicate.

How you can reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. Taxes. Security. Together. We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal information and that of any dependents. Don't routinely carry Social Security cards, and make sure your tax records are secure.

See Publication 4524, *Security Awareness for Taxpayers* to learn more.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

IRS IP PIN Opt-in Program

- IP PIN program helps prevent an identity thief from filing a tax return with your SSN
- Identity Protection PIN (IP PIN) is a six-digit number
- 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

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

Pub 5367 IP PIN Opt-in Program Flyer

Identity Protection PIN
Opt-In Program for Taxpayers

WHAT'S NEW You are now eligible to voluntarily get an Identity Protection PIN that will help protect you from tax-related identity theft.

What is the IP PIN?

The IP PIN is a 6-digit number assigned to eligible taxpayers. It helps prevent identity thieves from filing fraudulent tax returns with stolen Social Security numbers (SSNs). An IP PIN helps the IRS verify taxpayers' identities and accept their electronic or paper tax returns for processing. The IRS issues IP PINs to confirmed identity theft victims once their cases are resolved. This process is unchanged. What is new is that any taxpayers who wants an IP PIN, even if they are not victims of identity theft, may now obtain one.

About the IP PIN Opt-in Program

Here's what you need to know before applying for your IP PIN:
- This is a voluntary program.
- You must pass a rigorous identity verification process.
- Spouses and dependents are eligible for an IP PIN if they can verify their identities.
- An IP PIN is valid for a calendar year.
- You must obtain a new IP PIN each filing season, using the online tool.
- The IP PIN tool is unavailable generally mid-November through mid-January each year.
- Correct IP PINs must be entered on electronic and paper tax returns to avoid rejections and delays.

How to Get an IP PIN

The fastest, easiest and preferred way is by using the Get an IP PIN online tool. Here's how it works:
- Go to IRS.gov/IPPIN, select the Get an IP PIN tool, verify your identity and create an account
- Once you have a username, password and security code, enter the Get an IP PIN tool
- Your IP PIN will be revealed to you.

Can't pass online identity proofing?

There are alternatives but there will be a delay in obtaining an IP PIN. Here's how it works:
- File Form 15227 if you have a valid SSN or ITIN, an adjusted gross income of $72,000 or less and access to a telephone. An IRS assistor will call you, validate your identity and ensure that you receive an IP PIN the next filing season.
- If you are ineligible for Form 15227, call the IRS for in-person options.

IMPORTANT: The IRS will never email, text or call you to request your IP PIN. Do not reveal your IP PIN to anyone but your trusted tax software provider or tax preparer. Neither your provider nor preparer will ask for your IP PIN except to complete your tax return. Protect your IP PIN from theft, especially scams.

Pub 5477 IP PIN Opt-in Program Poster

For additional details, visit **IRS.gov/IPPIN**

The Identity Protection PIN is a six-digit number assigned to eligible taxpayers and is known only to the taxpayer and the IRS. It helps prevent identity thieves from filing fraudulent tax returns using a taxpayer's Social Security number.

About the IP PIN Opt-In Program:

- This is a **voluntary** program.
- Taxpayers must pass a rigorous identity verification process.
- Spouses and dependents are eligible for an IP PIN if they can verify their identities.
- An IP PIN is valid for a calendar year.
- Taxpayers must obtain a new IP PIN each filing season.
- Correct IP PINs must be entered on electronic and paper tax returns to avoid rejections and delays.

How to get an IP PIN:

Taxpayers who want an IP PIN should go to **IRS.gov/IPPIN** and use the Get an IP PIN tool.

Beware of scams to steal IP PINs

Taxpayers should never share their IP PIN with anyone but their trusted tax provider. The IRS will never call, text or email requesting a taxpayer's IP PIN.

2023 Dirty Dozen

1. IRS Warns about Employee Retention Credit claims; Aggressive promoters making offers too good to be true
2. IRS wraps up 2023 Dirty Dozen list; reminds taxpayers and tax pros to be wary of scams and schemes
3. Beware of abusive tax avoidance schemes
4. Watch out for schemes aimed at high-income filers; Charitable Trusts...
5. Watch out for Offer in Compromise "mills" promoters offering "pennies on a dollar".
6. IRS urges tax pros and other businesses to beware of spearphishing
7. Taking tax advice on social media can be bad news for taxpayers
8. IRS warns to stay clear of shady tax preparers; offers tips on choosing tax professionals
9. IRS warns of scammers using fake charities to exploit taxpayers
10. Watch out for third-party promoters of false fuel tax credit claims
11. IRS warns of scammers offering “help” to set up an Online Account
12. Watch out for scammers using email and text messages to try tricking people

Form **14242** (October 2016)	Department of the Treasury - Internal Revenue Service **Report Suspected Abusive Tax Promotions or Preparers**	OMB Number 1545-2219

Use Form 14242 to report a suspected abusive tax avoidance scheme and/or tax return preparers who promote such schemes. More information about tax avoidance schemes is available at www.irs.gov/scams. **CLAIM FOR REWARD:** To claim a reward for providing this information to the IRS, file Form 211, Application for Reward for Original Information.

Answer the following questions as accurately as possible. Fields on this form have been designed to expand as additional information in entered.

1. Describe the suspected tax scheme being promoted

2. How did you become aware of the promotion or promoter *(e.g., seminar, internet, email, TV, flyer, newspaper, magazine, friend, relative, etc.)*

3. When did you first learn about the tax promotion *(mm/dd/yyyy)*

4. Promoter/Preparer information *(if more than one promoter/preparer is involved, provide information on all)*

Name of Promoter(s)/Tax Preparer(s)

4. Promoter / Preparer information (if more than one promoter / preparer is involved, provide information on all). Name of Promoter(s) / Tax Preparer(s)

Social Security Number (SSN) and/or Preparer Tax Identification Number (PTIN)

Mailing address

Website

Telephone number

www.irs/SCAMS

IRS

Search

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

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

Home > File > Businesses and Self-Employed > Small Business and Self-Employed > Tax Scams How to Report Them

Tax Scams - How to Report Them

English

- Individuals
- International Taxpayers
- Businesses and Self-Employed
  - Small Business and Self-Employed
    - Employer ID Numbers
    - Business Taxes
    - Reporting Information Returns
    - Self-Employed

Participating in an illegal scheme to avoid paying taxes can result in imprisonment and fines, as well as the repayment of taxes owed with penalties and interest. If you become aware of any abusive tax scams, please report them to the appropriate contact below.

Reporting Tax Scams

Phishing Scams

Phishing is a scam typically carried out through unsolicited email and/or websites that pose as legitimate sites and lure unsuspecting victims to provide personal and financial information.

Report all unsolicited email claiming to be from the IRS or an IRS-related function to phishing@irs.gov . If you've experienced any monetary losses due to an IRS-related incident, please report it to the Treasury Inspector General Administration (TIGTA) and file a complaint with the Federal Trade Commission (FTC) through their Complaint Assistant to make the information available to investigators.

Related Topics

- Overview Abusive Tax Schemes
- Program to Shut Down Schemes and Scams
- Civil and Criminal Actions 1
- Listed Transactions
- How to Make an Offshore Voluntary Disclosure
- Abusive Return Preparer Criminal Investigation (CI)

Videos

- Tax Scams - Sound Too Good to be True (Video)

Questionable Return Preparers

- Requires payment in cash only and receipt.
- Guarantees a refund, or fees based on size of refund.
- Invents income to qualify their clients for tax credits.
- Claims fake deductions and/or credits to boost the size of the refund.
- Directs refunds into their bank account
- Doesn't have a Preparer Tax Identification Number (PTIN).
- Provides an unsigned return.

Tax Scams / Consumer Alerts | Internal Revenue Service (irs.gov)

- Employee Retention Credit scams and how to spot them
- Tax season is prime time for phone scams
- IRS, Security Summit partners remind families to make online safety a priority
- Charity Fraud Information
- Beware of OIC Mills – avoid costly promoters advertising settlement with the IRS for “pennies-on-the-dollar”
- Scam targets educational institutions, including students and staff
- Taxpayers should be on the lookout for new version of SSN scam
- Scams related to natural disasters
- New IRS impersonation email scam; reminds taxpayers the IRS does not send unsolicited emails
- IRS reminder: Tax scams continue year-round
- IRS warns of new phone scam using Taxpayer Advocate Service numbers
- IRS: Don’t be victim to a "ghost" tax return preparer
- IRS-Impersonation Telephone Scams

New Scams

- IRS, Security Summit partners warn taxpayers of new scam; unusual delivery service mailing tries to trick people into sending photos, bank account information | Internal Revenue Service
- FCC Smartphone Security Checker | Federal Communications Commission
- Tax Scams / Consumer Alerts | Internal Revenue Service (irs.gov)

TIP Sheet to Avoid Tax Time Scams

STAY SAFE ONLINE DURING TAX TIME

NATIONAL CYBERSECURITY ALLIANCE

IN COLLABORATION WITH

INTERNAL REVENUE SERVICE

Tax season can be a stressful time for many Americans, and scammers are waiting for you to slip up so they can steal your personal information, money and identity. The National Cyber Security Alliance (NCSA) and the Internal Revenue Service (IRS) want to help you stay safe online while filing your taxes with these best practices, tips, and resources.

DID YOU SPOT A SCAM OR PHISHING ATTEMPT?

You can help protect others by reporting it. Contact the following agencies to report a phishing or scam attempt:

- FTC - Report Fraud
- IRS - Report Tax Fraud
- IRS - Report Phishing to phishing@irs.gov

BEFORE YOU GET STARTED: PREPARE YOUR DEVICES

LOCK DOWN YOUR LOGIN

Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. MFA will fortify your online accounts by creating an extra layer of security, such as a unique one-time code sent to your phone. Most major email and online tax preparation services have this tool available.

UPDATE YOUR SOFTWARE

Before filing your taxes at home or work, be sure that all internet-connected devices –including PCs, smartphones and tablets – are running the most current versions of software to improve the performance and security of your devices.

BEWARE OF PUBLIC WI-FI

Public wireless networks are not secure. If you are filing your taxes online make sure you are doing it on a secure and personal network. We advise the use of a Virtual Private Network (VPN) any time you need to operate on Wi-Fi.

STAY SAFE ONLINE DURING TAX TIME

NATIONAL CYBERSECURITY ALLIANCE

IN COLLABORATION WITH

INTERNAL REVENUE SERVICE

THINK BEFORE SUPPLYING SENSITIVE INFORMATION

Unsolicited emails, calls, or texts that prompt you to click on a link or share valuable personal and financial information are very likely scams. With your personal data, online thieves can swindle funds and/or commit identity theft. Learn how to recognize a scam with the following tips:

IRS COMMUNICATIONS: REAL VS. FAKE

Be skeptical of any phone calls, emails, or texts claiming to be from the IRS, or other government agencies. Almost all contact from the IRS will be initiated via the U.S. Postal Service. They will only call once they have established a line of communication with you via physical mail first. The IRS will not demand you make an immediate payment to a source other than the U.S. Treasury.

Unscrupulous callers claiming to be federal employees can be very convincing by using fake names or phony ID numbers. If you are unsure if the caller is legitimate, hang up, look up the direct number for the agency online, and call that source to verify.

OTHER RED FLAGS

- **Requests for PII:** Personally Identifiable Information (PII) refers to any data that could potentially identify a specific individual.
  - For example: Bank account information, Social Security numbers, login credentials, mailing addresses
- **Urgency**: The sender uses an abnormal sense of urgency, or other scare tactics, to obtain information.
- **Attachments**: The message includes an attachment, such as a PDF. Never open attachments from a suspicious or unknown email address. It may download malware or viruses onto your device.

TIP: WHEN IN DOUBT, THROW IT OUT

If an email or seems suspicious, even if you think you know the source, it's best to just delete it. You can also report IRS, Treasury or tax-related phishing scams to phishing@irs.gov, then delete it.

Am I really talking to the IRS?

- If the IRS wants to examine your return, they will send you a letter first
- If you owe the IRS money, you will get notices in the mail
- IRS employees will have two forms of government issued ID
- An IRS employee will never demand you pay them cash, or debit cards, or threaten arrest

How to Know if it's Really the IRS Calling or Knocking on Your Door

Topics in the News
News Releases
Multimedia Center
Tax Relief in Disaster Situations
Inflation Reduction Act
Tax Reform
Taxpayer First Act
Tax Scams/Consumer Alerts
The Tax Gap
Fact Sheets
IRS Tax Tips
e-News Subscriptions
IRS Guidance

The IRS wants you to understand how and when the IRS contacts taxpayers, and help you determine whether a contact you may have received is truly from an IRS employee.

The IRS initiates most contacts through regular mail delivered by the United States Postal Service.

However, there are circumstances in which the IRS will call or come to a home or business. These include when a taxpayer has an overdue tax bill, a delinquent (unfiled) tax return or has not made an employment tax deposit. An IRS employee may also view assets or tour a business as part of a collection investigation, an audit or an ongoing criminal investigation.

Even then, taxpayers will generally first receive several letters (called "notices") from the IRS in the mail.

- **Audits**
- **Collection**
- **Criminal Investigation**
- **Beware of Impersonations**

Related Items

- Audits
- Collection Procedures: Filing or Paying Late
- Private Debt Collection
- Taxpayers can protect themselves from scammers by knowing how the IRS communicates

How to Know if it's Really the IRS Calling or Knocking on Your Door | Internal Revenue Service

Key Points

- Annual list of top Dirty Dozen tax scams
- IRS does not initiate contact by email, text messages or social media to ask for personal or financial data
- Report scams and theft to the appropriate authorities
- Don’t open Phishing links
- Create strong passwords
- IP PIN helps prevent identity theft
- Do not share your IP PIN

Resources

- IRS warning: Scammers work year-round; stay vigilant | IRS
- www.irs.gov/securitysummit
- Report Phishing | Internal Revenue Service (irs.gov)
- Publication 5367 (en-sp), Identity Protection PIN Opt-In Program for Taxpayers
- IRS wraps up 2023 Dirty Dozen list
- Tips to help taxpayers hire a reputable tax preparer
- Resources + Guides - National Cybersecurity Alliance (staysafeonline.org)
- Pub 4524 – Security Awareness for Taxpayers
- Pub 5027 – ID Theft Information for Taxpayers
- Pub 5367 – IP PIN Opt-in Program Flyer
- Pub 5477 – IP PIN Opt-in Program Poster


Questions

Thank You...