IRS

Tax scams/Consumer alerts

Thousands of people have lost millions of dollars and their personal information to tax scams. Scammers use the regular mail, telephone and email to set up individuals, businesses, payroll and tax professionals.

The IRS **doesn't initiate** contact with taxpayers by email, text messages or social media channels to request personal or financial information. Know the telltale signs of a scam and how to know if it's really the IRS.

Scams targeting taxpayers

New scam mailing related to unclaimed refunds

The IRS warns taxpayers to be on the lookout for a new scam mailing that tries to mislead people into believing they are owed a refund.

The new scheme involves a mailing coming in a cardboard envelope from a delivery service. The enclosed letter includes the IRS masthead with contact information and a phone number that do not belong to the IRS and wording that the notice is "in relation to your unclaimed refund."

Employee Retention Credit scams and how to spot them

The IRS reminded businesses and tax-exempt groups to watch out for telltale signs of misleading claims about the Employee Retention Credit (ERC), sometimes called the Employee Retention Tax Credit or ERTC. The IRS and tax professionals continue to see aggressive broadcast advertising, direct mail solicitations and online promotions involving the ERC. While the credit is real, aggressive promoters are misrepresenting and exaggerating who can qualify for the credit.

The IRS has issued many warnings about ERC schemes from third party promoters that charge large upfront fees or a fee based on the amount of the refund. And the promoters may not tell taxpayers that wage deductions claimed on the business' federal income tax return must be reduced by the amount of the credit.

Businesses, tax-exempt organizations and others thinking about applying for the ERC need to carefully review the official requirements for this credit before they claim it.

Filing season scams involving fake Form W-2 wages

The IRS warns taxpayers of new scams that urge people to use wage information on a tax return to claim false credits in hopes of getting a big refund.

Pandemic-related email scams

In a continuing twist on a common scam, the IRS, state tax agencies and tax industry warn tax professionals to beware of evolving phishing scams that use various pandemic-related themes to steal client data.

Charity fraud awareness

The Internal Revenue Service warns taxpayers to be wary of criminals soliciting donations and falsely posing as legitimate charities. When fake charities scam unsuspecting donors, the proceeds don't go to those who need the help and those contributing to these fake charities can't deduct their donations on their tax return.

Also see:

- IR-2022-180, IRS joins effort to fight charity fraud during international recognition week

Beware of OIC mills – avoid costly promoters advertising settlement with the IRS for "pennies-on-the-dollar"

The IRS reminds taxpayers to beware of promoters claiming their services are needed to settle with the IRS, that their debts can be settled for "pennies-on-the-dollar" or that there is a limited window of time to resolve tax debts through the Offer in Compromise (OIC) program. These promoters are often referred to as "OIC Mills." Find information on OIC Mills in the news release IRS "Dirty Dozen" list warns people to watch out for Offer in Compromise 'mills' where promoters claim their services are needed to settle IRS debts..

Scam targets educational institutions, including students and staff

The Internal Revenue Service warned of an ongoing IRS-impersonation scam that appears to primarily target educational institutions, including students and staff who have ".edu" email addresses.

- IR-2021-68, IRS warns university students and staff of impersonation email scam
- Tax Tip 2021-42, University students and staff should be aware of IRS impersonation email scam

Identity theft and unemployment benefits

The IRS urges taxpayers to be on the lookout for criminals seeking to steal their identities to file fraudulent claims for unemployment compensation.

Because unemployment benefits are taxable income, states issue Forms 1099-G, Certain Government Payments, to recipients and to the IRS to report the amount of taxable compensation received and any withholding. Box 1 on the form shows "Unemployment Compensation."

Taxpayers who received a Form 1099-G for 2020 unemployment compensation that they did not receive should take the steps outlined at Identity Theft and Unemployment Benefits.

Scams related to natural disasters

The IRS reminds taxpayers that criminals and scammers try to take advantage of the generosity of taxpayers who want to help victims of major disasters.

See:

- How to avoid fraud and scams after a disaster
- Tips to help taxpayers avoid post-disaster scams
- People should donate carefully after a disaster to avoid scams

IRS: Don’t be victim to a "ghost" tax return preparer

The IRS warns taxpayers to avoid unethical tax return preparers, known as ghost preparers. A ghost preparer is someone who doesn't sign tax returns they prepare. Not signing a return is a red flag that the paid preparer may be looking to make a quick profit by promising a big refund or charging fees based on the size of the refund.

IRS impersonation telephone scams

A sophisticated phone scam targeting taxpayers, including recent immigrants, has been making the rounds throughout the country. Callers make aggressive calls posing as IRS agents, using fake names and bogus IRS identification badge numbers in hopes of stealing taxpayer money or personal information. They may know a lot about their targets, and they usually alter the caller ID to make it look like the IRS is calling.

Victims are told they owe money to the IRS and it must be paid promptly through a gift card or wire transfer. Victims may be threatened with arrest, deportation or suspension of a business or driver’s license. In many cases, the caller becomes hostile and insulting. Victims may be told they have a refund due to try to trick them into sharing private information. If the phone isn't answered, the scammers often leave an “urgent” callback request.

See:

- Knowing how scammers pose as the IRS can help taxpayers protect themselves
- Taxpayers beware: Tax season is prime time for phone scams

Some thieves have used video **relay services** (VRS) to try to **scam** deaf and hard of hearing individuals. Taxpayers are urged not trust calls just because they are made through VRS, as interpreters don’t screen calls for validity. For details see the IRS video: Tax Scams via Video Relay Service.

Limited English Proficiency victims are often approached in their native language, threatened with deportation, police arrest and license revocation, among other things. IRS urges all taxpayers caution before paying unexpected tax bills. Note that the IRS doesn't:

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the IRS will first mail you a bill if you owe any taxes.
- Threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.
- Demand payment without giving you the opportunity to question or appeal the amount they say you owe.
- Ask for credit or debit card numbers over the phone.

Scams targeting tax professionals

Increasingly, tax professionals are being targeted by identity thieves. These criminals – many of them sophisticated, organized syndicates - are redoubling their efforts to gather personal data to file fraudulent federal and state income tax returns. The Security Summit has a campaign aimed at tax professionals: Protect Your Clients; Protect Yourself.

IRS, Security Summit partners urge tax pros to take actions to prevent data theft

The Security Summit consists of IRS, state tax agencies and the tax community, including tax preparation firms, software developers, payroll and tax financial product processors, tax professional organizations and financial institutions.

The Security Summit provides awareness campaigns throughout the year. These include:

- Protect Your Clients; Protect Yourself
- Protect Your Clients; Protect Yourself — Summer 2023
- Taxes. Security. Together.

- National Tax Security Awareness Week

Also see:

- Latest spearphishing scams target tax professionals
- Security Summit: Identity Protection PINs provide an important defense against tax-related identity theft
- IRS Security Summit renews warnings for tax pros to guard against identity theft amid continued threats
- IRS, Summit partners issue urgent EFIN scam alert to tax professionals
- During National Cybersecurity Month, IRS and Security Summit Partners offer tips
- How to Maintain, Monitor and Protect Your EFIN
- Security Summit: Tell-tale signs of identity theft tax pros should watch for
- Security Summit: Tax pros should remain vigilant against phishing emails and cloud-based attacks
- Security Summit warns tax pros of evolving email and cloud-based schemes to steal taxpayer data

Soliciting Form W-2 information from payroll and human resources professionals

The IRS has established a process that will allow businesses and payroll service providers to quickly report any data losses related to the W-2 scam currently making the rounds. If notified in time, the IRS can take steps to prevent employees from being victimized by identity thieves filing fraudulent returns in their names. There also is information about how to report receiving the scam email.

Report these schemes

- Email dataloss@irs.gov to notify the IRS of a W-2 data loss and provide contact information. In the subject line, type "W2 Data Loss" so that the email can be routed properly. Do not attach any employee personally identifiable information.
- Email the Federation of Tax Administrators at statealert@taxadmin.org to learn how to report victim information to the states.
- Businesses/payroll service providers should file a complaint with the FBI's Internet Crime Complaint Center (IC3.gov). Businesses/payroll service providers may be asked to file a report with their local law enforcement.
- Notify employees so they may take steps to protect themselves from identity theft. The FTC's identitytheft.gov provides general guidance.
- Forward the scam email to phishing@irs.gov.
- See more details at Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers.

Employers are urged to put protocols in place for the sharing of sensitive employee information such as Forms W-2. The W-2 scam is just one of several new variations that focus on the large-scale thefts of sensitive tax information from tax preparers, businesses and payroll companies.

Tax professionals who experience a data breach also should quickly report the incident to the IRS. See details at Data Theft Information for Tax Professionals.

See:

- Dirty Dozen: Taking tax advice on social media can be bad news for taxpayers; schemes circulating involving tax forms

Surge in Email, Phishing and Malware Schemes

Schemes

Phishing (as in "fishing for information") is a scam where fraudsters send e-mail messages to trick unsuspecting victims into revealing personal and financial information that can be used to steal the victims' identity.

The IRS has issued several alerts about the fraudulent use of the IRS name or logo by scammers trying to gain access to consumers' financial information to steal their identity and assets.

Scam emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. These phishing schemes may seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information.

Be alert to bogus emails that appear to come from your tax professional, requesting information for an IRS form. IRS doesn't require Life Insurance and Annuity updates from taxpayers or a tax professional.

Variations can be seen via text messages. The IRS is aware of email phishing scams that include links to bogus web sites intended to mirror the official IRS website. These emails contain the direction "you are to update your IRS e-file immediately." These emails are not from the IRS.

The sites may ask for information used to file false tax returns or they may carry malware, which can infect computers and allow criminals to access your files or track your keystrokes to gain information.

Unsolicited email claiming to be from the IRS, or from a related component such as EFTPS, should be reported to the IRS at phishing@irs.gov.

For more information, visit the IRS's Report Phishing webpage.

Fraudsters posing as Taxpayer Advocacy Panel

Some taxpayers receive emails that appear to be from the Taxpayer Advocacy Panel (TAP) about a tax refund. These emails are a phishing scam, trying to trick victims into providing personal and financial information. Do not respond or click any link. If you receive this scam, forward it to phishing@irs.gov and note that it seems to be a scam phishing for your information.

TAP is a volunteer board that advises the IRS on systemic issues affecting taxpayers. It never requests, and does not have access to, any taxpayer's personal and financial information.

Related information

How to report tax-related schemes, scams, identity theft and fraud

To report tax-related illegal activities, refer to Tax Scams - How to Report Them. You should also report instances of IRS-related phishing attempts and fraud to the Treasury Inspector General for Tax Administration at 800-366-4484.

Taxpayers who experience tax-related identity theft may wonder when they should file a Form 14039, Identity Theft Affidavit.

- When to file a Form 14039, Identity Theft Affidavit

Additional scam-related information

- Criminal Investigation's Tax Fraud Alerts
- State ID Theft Resources - State information on what to do if you or your employees are victims of identity theft.
- IRS Dirty Dozen – The annually compiled list enumerates a variety of common scams that taxpayers may encounter.

IRS YouTube videos

- Tax Scams via Video Relay Service in ASL

Page Last Reviewed or Updated: 04-Mar-2024