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, or 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. Recognize the telltale signs of a scam. See also: How to know it's really the IRS calling or knocking on your door

Scams Targeting Taxpayers

Scam Alert: IRS Urges Taxpayers to Watch Out for Erroneous Refunds; Beware of Fake Calls to Return Money to a Collection Agency

The Internal Revenue Service today warned taxpayers of a quickly growing scam involving erroneous tax refunds being deposited into their bank accounts. The IRS also offered a step-by-step explanation for how to return the funds and avoid being scammed.

Following up on a Security Summit alert issued Feb. 2, the IRS issued this additional warning about the new scheme after discovering more tax practitioners' computer files have been breached. In addition, the number of potential taxpayer victims jumped from a few hundred to several thousand in just days. The IRS Criminal Investigation division continues its investigation into the scope and breadth of this scheme.

These criminals have a new twist on an old scam. After stealing client data from tax professionals and filing fraudulent tax returns, these criminals use the taxpayers' real bank accounts for the deposit.

Thieves are then using various tactics to reclaim the refund from the taxpayers, and their versions of the scam may continue to evolve.

- See IR-2018-27

IRS-Impersonation Telephone Scams

A sophisticated phone scam targeting taxpayers, including recent immigrants, has been making the rounds throughout the country. Callers claim to be IRS employees, using fake names and bogus IRS identification badge numbers. They

The Newsroom Topics

- Multimedia Center
- Noticias en Español
- IRS Radio PSAs
- Tax Scams Consumer Alerts
- The Tax Gap
- Fact Sheets 2017
- IRS Tax Tips
- Latest News

Social Media

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.

- Please See: Consumer Alert: Scammers Change Tactics, Once Again

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. Please see: IRS Alerts Taxpayers with Limited English Proficiency of Ongoing Phone Scams. 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.

Recent scams targeting the tax professional community include:

- Tax Professionals Urged to Step Up Security as Filing Scheme Emerges
- Tax Professionals Warned of e-Services Scam.
- Tax Professionals Warned of New Scam to "Unlock" Tax Software Accounts.
- A phishing scheme mimicking software providers targets tax professionals.
- Criminals target tax professionals to steal data such as PTINs, EFINs or e-Service passwords.
- Bogus email asks tax professionals to update their IRS e-services portal information and Electronic Filing Identification Numbers (EFINs).

- See: IRS Warns Tax Preparers to Watch out for New Phishing Scam; Don't Click on Strange Emails or Links Seeking Updated Information

Tax professionals should review Publication 4557, Safeguarding Taxpayer Data, A Guide for Your Business, which provides a checklist to help safeguard information and enhance security.

See also: Identity Theft Information for Tax Professionals.

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 www.identitytheft.gov provides general guidance.
- Forward the scam email to phishing@irs.gov.
- See more details at Form W2/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.

Also see:

- IRS, States and Tax Industry Warn Employers to Beware of Form W-2 Scam; Tax Season Could Bring New Surge in Phishing Scheme
- IRS, States and Tax Industry Renew Alert about Form W-2 Scam Targeting Payroll, Human Resource Departments
- IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s

Surge in Email, Phishing and Malware 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. Beware of this scam.

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 web site. 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.

For more details, see:

- Consumer Alert: IRS Warns Taxpayers, Tax Pros of New Email Scam Targeting Hotmail Users
- IRS Warns Seniors to Beware of Calls by Criminals Impersonating the IRS
- Phishing Remains on the IRS "Dirty Dozen" List of Tax Scams for the 2017 Filing Season

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 web page.

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.

Additional Recent Tax Scams

Heightened Fraud Activity as Filing Season Approaches

- See: Security Summit Partners Warn Tax Pros of Heightened Fraud Activity as Filing Season Approaches

Email Scam Targeting Hotmail Users

- See: Consumer Alert: IRS Warns Taxpayers, Tax Pros of New Email Scam Targeting Hotmail Users

FBI Themed Ransomware Scam

- See: IRS Issues Urgent Warning to Beware IRS FBI Themed Ransomware Scam

Last-Minute Email Scams

- See: IRS, States and Tax Industry Warn of Last-Minute Email Scams

Fictitious "Federal Student Tax" scam targeting students and parents and demanding payment.

- See: IRS Warns of Back-to-School Scams; Encourages Students, Parents, Schools to Stay Alert
- See: IRS Warns of Latest Scam Variation Involving Bogus "Federal Student Tax"

Automated calls requesting tax payments in the form of iTunes or other gift cards.

- See: IRS Warns Taxpayers of Summer Surge in Automated Phone Scam Calls; Requests for Fake Tax Payments Using iTunes Gift Cards

Pretending to be from the tax preparation industry.

- See: Consumers Warned of New Surge in IRS E-mail Schemes during 2016 Tax Season; Tax Industry Also Targeted

How to Report Tax-Related Schemes, Scams, Identity Theft and Fraud

To report tax-related illegal activities, refer to our chart explaining the types of activity and the appropriate forms or other methods to use. You should also report instances of IRS-related phishing attempts and fraud to the Treasury Inspector General for Tax Administration at 800-366-4484.