Tax Scams/Consumer Alerts

If it sounds too good to be true, it probably is! In recent years, thousands of people have lost millions of dollars and their personal information to tax scams and fake IRS communication. This page looks at the scams affecting individuals, businesses, and tax professionals and what do if you if you spot a tax scam.

REMEMBER: The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information. In addition, IRS does not threaten taxpayers with lawsuits, imprisonment or other enforcement action. Being able to recognize these tell-tale signs of a phishing or tax scam could save you from becoming a victim.

Information for Taxpayers

IRS-Impersonation Telephone Scams

An aggressive and sophisticated phone scam targeting taxpayers, including recent immigrants, has been making the rounds throughout the country. Callers claim to be employees of the IRS, but are not. These con artists can sound convincing when they call. They use fake names and bogus IRS identification badge numbers. 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 pre-loaded debit card or wire transfer. If the victim refuses to cooperate, they are then threatened with arrest, deportation or suspension of a business or driver's license. In many cases, the caller becomes hostile and insulting. Or, 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.

Note that the IRS will never:

- 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 immediately bring in local police or other law-enforcement groups to have you arrested for not paying.
- Demand that you pay taxes 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.

Remember: Scammers Change Tactics – Aggressive and threatening phone calls by criminals impersonating IRS agents remain a major threat to taxpayers, but variations of the IRS impersonation scam continue year-round and they tend to peak when scammers find prime opportunities to strike.

Surge in Email, Phishing and Malware Schemes

The IRS saw an approximate 400 percent surge in phishing and malware incidents in the 2016 tax season.

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 can ask taxpayers about a wide range of topics. Emails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information.

Variations of these scams can be seen via text messages, and the communications are being reported in every section of the country.

When people click on these email links, they are taken to sites designed to imitate an official-looking website, such as IRS.gov. The sites ask for Social Security numbers and other personal information, which could be used to help file false tax returns. The sites also may carry malware, which can infect people's computers and allow criminals to access your files or track your keystrokes to gain information.

For more details, see:

- IR-2016-28, Consumers Warned of New Surge in IRS Email Schemes during 2016 Tax Season; Tax Industry Also Targeted
- IR-2016-15, Phishing Remains on the IRS “Dirty Dozen” List of Tax Scams for the 2016 Filing Season

Email Phishing Scam: "Update your IRS e-file"

The IRS is aware of email phishing scams that appear to be from the IRS and include a link to a bogus web site intended to mirror the official IRS web site. These emails contain the direction “you are to update your IRS e-file immediately.” The emails mention USA.gov and IRSgov (without a dot between "IRS" and "gov"), though notably, not IRS.gov (with a dot). Don’t get scammed. These emails are not from the IRS.

What do you do if you get these messages?

- Do not respond to the email or click on the links.
- Instead, they should forward the scam emails to the IRS at phishing@irs.gov.

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

Remember, the IRS does not initiate contact with taxpayers by email to request personal or financial information.

Tax Refund Scam Artists Posing as Taxpayer Advocacy Panel

According to the Taxpayer Advocacy Panel (TAP), taxpayers are receiving emails that appear to be from TAP about a tax refund. These emails are a phishing scam, where unsolicited emails which seem to come from legitimate organizations — but are really from scammers — try to trick unsuspecting victims into providing personal and financial information. Do not respond or click the links in them. If you receive an email that appears to be from TAP regarding your personal tax information, please forward it to phishing@irs.gov and note that it seems to be a scam email 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 such as Social Security and PIN numbers or passwords and similar information for credit cards, banks or other financial institutions.

Watch Out for These Recent Tax Scams

Scammers are constantly identifying new tactics to carry out their crimes in new and unsuspecting ways. In recent years, the IRS has seen scammers use a variety of schemes to fool taxpayers into paying money or giving up personal information. Some of these include:

An email scam that uses a corporate officer’s name to request employee Forms W-2 from company payroll or human resources departments - see IR-2017-10

Sending fake emails purporting to contain an IRS tax bill related to the Affordable Care Act — see IR-2016-123

IRS reminds taxpayers against telephone scammers targeting students and parents during the back-to-school season - see IR-2016-107

Imitating software providers to trick tax professionals — see IR-2016-103

Demanding fake tax payments using iTunes gift cards — see IR-2016-99

IRS warns taxpayers about bogus phone calls from IRS impersonators demanding payment for a non-existent tax, the “Federal Student Tax.” - see IR-2016-81

IRS warns taxpayers of a phishing scam targeting Washington D.C., Maryland and Virginia residents where the email scammers are citing tax fraud and trying to trick victims into verifying "the last four digits of their social security number" - see IR-2016-55

"Verifying" tax return information over the phone — see IR-2016-40

Soliciting W-2 information from payroll and human resources professionals — see IR-2016-34.

Pretending to be from the tax preparation industry — see IR-2016-28

Don't fall victim to tax scams. Remember — if it sounds too good to be true, it probably is.

Additional scam-related information:

- IRS Security Awareness Tax Tips

Education is the best way to avoid the pitfalls of these "too good to be true" tax scams. For more information, see:

- Tax Scams — How to Report Them
- Criminal Investigation's Tax Fraud Alerts

Information for 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 launched a campaign aimed at increasing awareness among tax professionals: Protect Your Clients; Protect Yourself.

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

Phony Arguments

No matter how some things are sliced, they're still baloney. If someone tells you that you don't have to pay taxes, check out The Truth About Frivolous Tax Arguments, where some of the more common false legal arguments made by those opposed to compliance with the federal tax laws are addressed. The page explains and rejects each contention, deals with frivolous arguments encountered in collection due process cases and illustrates penalties imposed on those pursuing frivolous cases.

See also IR-2016-27, Frivolous Tax Arguments Completes the IRS "Dirty Dozen" List of Tax Scams for the 2016 Filing Season

---

Identity Theft Scams

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 in order to steal their identity and assets. Scammers use the regular mail, telephone, fax or email to set up their victims. When identity theft takes place over the web (email), it is called phishing.

The IRS does not initiate taxpayer communications through email. Unsolicited email claiming to be from the IRS, or from an IRS-related component such as EFTPS, should be reported to the IRS at phishing@irs.gov.

Additionally, clicking on attachments to or links within an unsolicited email claiming to come from the IRS may download a malicious computer virus onto your computer.

Security Summit Learn more about how the IRS, representatives of the software industry, tax preparation firms, payroll and tax financial product processors and state tax administrators are working together to combat identity theft and refund fraud.

Learn how to protect your personal information.

Reporting Tax-Related Schemes, Scams, Identity Theft and Fraud

To report the various types of tax-related illegal activities, refer to our chart explaining the types of activity and the appropriate forms or other methods to use.

You may also report instances of IRS-related phishing attempts and fraud to the Treasury Inspector General for Tax Administration at 800-366-4484.

National Tax Security Awareness Week

The week (Dec. 5-9, 2016) featured a series of consumer warnings and tips released daily and featured on the Security Summit web page and a one-page Publication 4524, Security Awareness for Taxpayers.

See also:

- National Tax Security Week Concludes; IRS, Security Summit Partners Continues Work to Protect Taxpayers in 2017 (IR-2016-166)
- IRS Warns Taxpayers of Numerous Tax Scams Nationwide; Provides Summary of Most Recent Schemes (IR-2016-164)
- Protect Your Clients: Security Summit Partners Warn Tax Pros of Cybercriminals, Launch New Awareness Tips (IR-2016-163)
- IRS, Security Summit Partners Remind Taxpayers to Recognize Phishing Scams (IR-2016-160)
- IRS, Security Summit Partners, Remind Taxpayers to Protect Themselves Online (IR-2016-158).
- IRS and its Security Summit partners announce "National Tax Security Awareness Week." (IR-2016-156).

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

IRS Security Awareness Tips

IRS YouTube Videos on Tax Scams

- Tax Scams: English | Spanish | ASL
- Phishing-Malware: English | Spanish | ASL

Page Last Reviewed or Updated: 25-Jan-2017