Scams Targeting 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.

Surge in Email, Phishing and Malware Schemes

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 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. 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). These emails are not from the IRS.

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:

- Phishing Remains on the IRS “Dirty Dozen” List of Tax Scams for the 2017 Filing Season
- Consumers Warned of New Surge in IRS Email Schemes during 2016 Tax Season; Tax Industry Also Targeted
- 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”

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

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.