Huntington Welcome.℠

Help be prepared against fraud this tax season

Tax season is an ideal time for scam artists and cybercriminals to steal personal data or use information they already have. With your social security number, thieves can file a fraudulent return in your name and collect the refund. They can also use or sell your personal information to commit other crimes.

To help avoid tax-related identity theft, taxpayers are encouraged to file their taxes early, regularly monitor their credit reports and be suspicious of any request that asks for their personal information.

COMMON TAX SCAMS

Email Phishing

Email phishing scams are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies.

Be alert to emails from the Taxpayer Advocacy Panel (TAP), which is a volunteer board that advises the IRS on systemic issues affecting taxpayers. TAP never requests, and does not have access to, any taxpayer's personal and financial information.

Phone Phishing

Phone scams from callers claiming to be IRS employees, using fake names and ID numbers that target taxpayers and recent immigrants. They may know a lot about their targets, and they usually alter the caller ID to make it look like the IRS is calling.

Text Smishing

Variations of phishing emails come by text messages that link to fake websites intended to mirror the official IRS website.

Remember: Huntington will never ask you for account numbers or passwords by phone, email or text.

Learn more about phishing at huntington.com/Privacy-Security.

HOW TO REPORT TAX FRAUD

1. Forward any suspicious tax-related email to phishing@irs.gov.
2. Call the IRS Identity Protection Specialized Unit at (800) 908-4490 or visit https://www.irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity.
3. File a complaint with the Federal Trade Commission (FTC) at identitytheft.gov.
4. Consider placing a fraud alert on your credit records with the three major credit bureaus at equifax.com, transunion.com and experian.com.
5. Contact your bank and any other financial institutions, and close any financial or credit accounts that might have been opened without your permission or compromised by identity thieves.

$961 million

dollars in fraudulent refunds caught by the IRS as of March 4, 2017[1]

34%

of reported identity theft complaints in 2016 were employment and tax-related [2]

399K

identity theft complaints filed with the FTC in 2016[3]

[1] Source: Treasury Inspector General for Tax Administration, *Interim Results of the 2017 Filing Season*

[2] Source: Federal Trade Commission, *Tax Identity Theft Awareness Week has an event for you*

[3] Source: Federal Trade Commission, *FTC Releases Annual Summary of Consumer Complaints*

Turn over for additional tips.

How to Help Avoid Tax Scams

Legitimate companies will not ask you to provide or verify sensitive information through non-secure means, such as email or text.

- **File your taxes as early as possible during tax season.** Fraudsters using stolen identities tend to file false returns early hoping to obtain refunds before the legitimate taxpayer files their return.
- **If you aren't required to file a tax return, consider filing anyway to prevent someone else from filing in your name.** This will also help alert you in case someone has already filed a fraudulent return in your name.
- **Before giving out information**, verify email or other requests that appear to come from a tax professional, financial institution or government entity.
- **Scammers often may have extensive information about a person**, and the caller ID on your phone may actually show a local law enforcement agency or similar official-looking name.
- **Only give out your personal information when absolutely necessary**—especially on websites and social media sites—and keep track of who you give it to. This could be helpful in determining the source of a breach of personally identifiable information if you become a victim.

How the IRS Contacts Taxpayers

- **The IRS will not initially contact you by phone call, text message, social media or e-mail** to ask for your personal or financial information or to obtain payment for a tax bill. The government loves a paper trail. The IRS will write to you first, possibly multiple times. If you are unsure about a tax bill, call the IRS at (800) 829-1040.
- **The IRS will not give you an ultimatum** to pay up immediately or demand that you wire money. The IRS also won't call to congratulate you for getting a refund.
- **The IRS will not demand** that the taxpayer pay without the opportunity to question or appeal.
- **The IRS will not threaten** to send police, immigration officers or other law enforcement to arrest you.
- **The IRS will not ask you** to pay your debt using iTunes gift cards or any other type of gift or debit cards. They also will not ask you to pay with alternative currency, such as bitcoin.
- **In the case of a personal visit from someone claiming to be from the IRS or other government entity,** check for official credentials in the form of a pocket commission and HSPD-12 card. No one making a personal visit will demand immediate payment, especially to a source other than the U.S. Treasury.

Contact Huntington

If you receive a suspicious email, call or text claiming to be from Huntington, or think your account data has been compromised, let us know. We'll work with you to determine the legitimacy of suspicious messages and account activity.

PHONE: **(800) 480-2265**

EMAIL: **ReportFraud@huntington.com**

For more information about phishing or your privacy and security, go to **huntington.com/Privacy-Security**