Income Tax Scams and How to Protect Yourself

From Associated Bank

SUMMARY
Income tax scams are attempts to steal your money by impersonating the IRS or promising fake tax benefits, or by filing tax returns (to obtain refunds) using your personal identity.

Cybercriminals use email, phone calls, text messages and even fake tax preparers to trick people into providing their sensitive information.

The IRS and legitimate tax services will never threaten you with arrest or legal action over the phone or by email.

Common Types of Tax Scams

1. **Traditional phishing scams:** Fraudulent emails, text messages or phone calls requesting personal identity information. Scammers attempt to trick you into clicking a suspicious link, downloading a malicious attachment or even scanning a fake QR code to steal personal sensitive information or infect your device with malicious software. These attempts may appear unrelated to tax preparation or the tax season, but may enable the scammer to steal your identity and file bogus tax returns in your name. Remember: The IRS, the Social Security Administration, Medicare and your financial institutions will never call asking for your social security number or other sensitive information.

2. **IRS impersonation calls:** Scammers pose as IRS agents demanding immediate payment or threatening arrest, legal action or seizure of assets. The IRS with never call to demand payment over the phone or threaten you with law enforcement arrest.

3. **Identity theft and fake tax returns:** Scammers use stolen social security numbers to file fraudulent tax returns in order to obtain refunds. Victims only discover the fraud when they try to file and get rejected.

4. **Fake tax preparers:** Unscrupulous preparers file false returns or steal clients' refunds. Some charge fees based on a percentage of the refund or ask clients to sign blank tax returns.

5. **Refund and stimulus check scams:** Scammers claim you're entitled to additional refunds or stimulus checks. They ask for personal information to "process" the payment but instead steal your identity.

How to Protect Yourself

- **File early:** Reduce the risk of identity thieves filing a return in your name.
- **Use secure tax software:** Ensure your tax software is reputable and up to date, or use a professional tax return preparer.

- **Verify tax preparers:** Check credentials using the IRS's Directory of Federal Tax Return Preparers.
- **Shred sensitive documents:** Prevent identity theft by securely disposing old tax documents, and anything else that contains Social Security, Medicare or financial account numbers. If you don't have a shredder, local UPS stores will shred your documents for $1 per pound.
- **Enable multi-factor authentication:** Add an extra layer of security to your tax, financial and banking accounts. This is highly recommended! Multi-factor authentication (also called two-factor authentication) will send a code to you via text message or phone call when you try to access your account online. You then enter that code to complete your access.
- **Monitor your tax account:** Check for unauthorized filings at https://www.irs.gov/account.

What should you do if you suspect a tax scam?

Scammers are constantly evolving their tactics, so staying informed is your best defense. When in doubt, pause, verify the source and report any suspicious activity to the IRS. By staying alert, you can protect yourself and your family from tax scams.

For more information about how to protect yourself from cybercrime, visit
https://milwaukeequakers.org/cybersecurity/