Cybersecurity for Tax Season: Protect Your Identity and Refund

Tax season brings enough stress without adding scammers to the mix. But the reality is that criminals ramp up attacks in the first few months of the year, often impersonating the IRS or trusted services like H&R Block and TurboTax. By adopting smart security habits, you can protect your data and ensure your tax refund goes where it belongs—your bank account.

Essential cybersecurity tips for tax season

1. File your taxes early.

Here's our top tip for tax time cybersecurity: file your taxes as soon as possible. Filing quickly reduces the risk of tax fraud. A common scam is for criminals to try to submit fraudulent tax returns using stolen Social Security numbers to claim refunds. Employers must send out W-2s and 1099 forms by January 31, so once you have your documents, don't delay. If a criminal files before you do, reclaiming your refund is a lengthy and stressful process. If you are in this situation, contact the IRS as soon as possible.

2. Secure your return with an IRS IP PIN.

The IRS offers an Identity Protection PIN (IP PIN)—a six-digit code that prevents unauthorized tax filings using your Social Security number. You can apply for an IP PIN through the IRS website. While we recommend that everyone signs up for an IP PIN, this is especially true if your SSN has been exposed in a data breach. Once issued, this number should be kept private and used only when filing your return.

3. Enable multifactor authentication (MFA).

Use MFA on all accounts related to your taxes, including your IRS account, tax preparation software, and any account with a financial institution, like your bank. MFA requires an additional verification step, like a scan of your face, making it much harder for hackers to gain access—even if they have your password.

4. Look out for tax scams and phishing.

Cybercriminals commonly impersonate the IRS, tax preparers, and financial institutions. Be on high alert for phishing emails, scammy phone calls, and fake websites designed to steal your personal information.

Red flags of a tax phishing scam:

- Unsolicited IRS communications: The IRS never initiates contact via email, text, or social media.
- Urgency and threats: Scammers use scare tactics, like threats of arrest or financial penalties, to pressure you into immediate action. They play on your emotions and use a sense of urgency to try to get you to not think about what you're doing.

- Requests for sensitive data: Don't respond to emails or calls asking for your Social Security number, banking details, or login credentials. The IRS and financial institutions don't use these methods to transmit sensitive data because they are not secure.
- Attachments or links: Phishing emails typically contain malicious links or attachments that can install malware on your device. Think before you click.

5. Ask about your tax preparer's cybersecurity practices.

If you use a tax professional, make sure they take cybersecurity seriously. Ask these critical questions and take note of their responses: How do you protect client data? Do you use encrypted portals for document sharing? Who has access to my information within your firm? How do you back up sensitive tax records? How long do you store tax records? Encryption for protecting data, documents, and communications is critical, and you want them to limit who can access your records. You also want a tax service that uses encrypted, secure backup systems and only stores your records for three to seven years.

6. Safely exchange tax documents.

Avoid emailing tax documents as regular attachments. Instead, use encrypted email services or a secure file-sharing portal your tax preparer provides. If mailing documents, send them through a trusted courier service with tracking options.

7. Back up your tax records.

Make digital and physical backups of your tax documents. Store electronic copies in an encrypted cloud storage service or an external hard drive (or both!) and keep printed copies in a secure location. The IRS generally recommends retaining tax records for three years, but depending on your situation, you may need to keep them longer.

8. Report scams to the authorities.

If you think you are the target of a tax scam, report it immediately.

- IRS victims of identity theft: IRS Identity Theft Central
- Treasury Inspector General for Tax Administration (TIGTA): Report IRS-related Impersonation
- IRS, Treasury, and tax-related online scams: Report Phishing
- IRS CI: Report Tax Fraud
- FTC: Report Fraud
- IC3: Report Cybercrime

Protect yourself from tax time scams

By staying vigilant and following these cybersecurity best practices, you can protect your identity, secure your tax return, and reduce the risk of fraud. Don't let cybercriminals make tax season more stressful than it already is! Stay safe online and file with confidence!
