west protect℠

SAFE

Security Awareness For Everyone

Tip Sheet

Tax season can be a frantic time for many of us, and the increase in tax-related scams doesn't make it any calmer. In 2023, the IRS identity theft detection systems flagged over 1.1 million tax returns as potentially fraudulent, with associated refunds totaling over $6 billion. Cybercriminals love to impersonate government agencies, like the IRS. Still, by adopting some secure behaviors, you can stay safe while filing your taxes. The following best practices can drastically improve your security during tax season:

1. FILE EARLY

The sooner you file, the less time cybercriminals have to file a fake return and try to nab your refund.

2. USE AN IP PIN

You can get a unique Identity Protection PIN (IP PIN) from the IRS to secure your online tax information. It's a six-digit number that prevents someone else from filing a tax return using your Social Security number; it's shared just between you and the IRS. If you've been alerted that your Social Security number was part of a data breach, you should apply for an IP PIN.

3. ENABLE MFA

Another best practice is to use multi-factor authentication (MFA) wherever possible, including any account related to your taxes. Even if hackers get ahold of your password, MFA keeps your accounts locked.

4. DON'T FEAR THE SCAMMER

But do stay alert! You might receive phishing messages trying to scare you into action before you can think. Scammers can be convincing at impersonating IRS employees using fake names, spoofing telephone numbers, and sending official-looking messages. Remember, the IRS will never email, text, or DM you. If you get a call and are unsure, hang up, look up the direct number for the agency, then call and verify.

Red Flags to watch for. Impersonating the IRS can take the usual phishing scams to another level of panic when you should stay calm.

Requests for data: Be highly suspicious of any communications that ask you to provide personal information such as bank account information, Social Security numbers, login credentials, or mailing addresses.

Urgency: Scammers use an abnormal sense of urgency and other scare tactics to obtain information. Their goal is to make you panic and stop thinking clearly.

Attachments: Watch out for messages that include an attachment, and never open attachments from suspicious or unknown email addresses. It could download malware or viruses to your device. Just because it may be password-protected doesn't mean it's from a secure source, or you can trust it. Always verify the email by calling a published number.

Impersonating tax preparers: Along with the IRS, scammers imitate popular tax programs like TurboTax and H&R Block. These companies will never contact you through phone, email, or text asking for your login information or asking you to give them an MFA code you didn't request.