



WV Executive Branch Privacy Tip

April 2023

Tax Season Security Tips

Tax season is a stressful time for most of us, and scammers add even more anxiety to this frantic season.

There is an uptick in phishing, scamming, and other online fraud during tax time, and lots of bad actors love to catfish as the Internal Revenue Service. By following some simple best practices, though, you can keep the hackers' mitts off your refund.

RED FLAGS OF IRS SCAMS:

- Requests for data: Be extremely suspicious of any communications that ask you to provide personal information such as bank account information, Social Security numbers, login credentials, or mailing addresses. Cybercriminals will often impersonate the IRS in phishing campaigns.
- 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 any message that includes an attachment, such as a PDF. Never open attachments from a suspicious or unknown email address. It may download malware or viruses onto your device.
- Phishing as tax preparers: Along with the IRS, scammers will also imitate popular tax programs like TurboTax and H&R Block to try to snag your financial information. These companies will never contact you through phone, email, or text asking for your login information, or for you to give them an MFA code that you didn't request.

REPORT SCAMS

If you think you are the victim of a tax scam, report it right away. The sooner you report the incident, even if you aren't totally sure, the better your chances of recovering your cash.

- 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](#)

For more information on how to stay safe online, please visit <https://staysafeonline.org/>



Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.