Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Follow these tips to protect data when shopping online

Tax Tip 2018-185
December 3, 2018

The IRS reminds holiday shoppers to protect their tax and financial data from identity thieves. All it takes is a few extra steps to prevent cybercriminals from stealing sensitive data, such as financial account information, Social Security numbers, and credit card information. Thieves could use this data to file a fraudulent tax return in 2019.

This tip is part of National Tax Security Awareness Week. The IRS is partnering with state tax agencies and its partners in the Security Summit to remind to taxpayers and tax professionals about the importance of protecting data.

Cybercriminals want to turn stolen data into quick cash. They do this by draining financial accounts, charging credit cards, creating new credit accounts or even using stolen identities to file a fraudulent tax return for a refund.

Here are seven steps taxpayers can follow to help protect their accounts and their money:

- **Avoid unprotected Wi-Fi.** Unprotected public Wi-Fi hotspots may allow thieves to view transactions.
- **Shop at familiar online retailers.** Generally, sites using the “s” designation in “https” at the start of the URL are secure. User can also look for the “lock” icon in the browser’s URL bar. That said, some thieves can get a security certificate, so the “s” may not always vouch for the site’s legitimacy. Beware of purchases at unfamiliar sites or clicks on links from pop-up ads.
- **Learn to recognize and avoid phishing emails.** Thieves send these emails, posing as a trusted source, such a financial institution. or the IRS. The criminal’s goal is to entice users to open a link or attachment. The link may take users to a fake website that will steal usernames and passwords. An attachment may download malware that tracks keystrokes.
- **Keep a clean machine.** This applies to computers, phones and tablets. Taxpayers should use security software to protect against malware that may steal data and viruses that may damage files.
- **Use passwords that are strong, long and unique.** Experts suggest a minimum of 10 characters but longer is better. People should also avoid using a specific word in the password. They should also use a combination of letters, numbers and special characters.
- **Use multi-factor authentication when available.** This means users may need a security code, usually sent as a text from a financial institution or email provider to a mobile phone. People use this code in addition to usernames and passwords.
- **Encrypt and password-protect sensitive data.** If keeping financial records, tax returns or any personally identifiable information on computers, this data should be encrypted and protected by a strong password.

More Information:
Taxes. Securty. Together
Publication 4524, Security Awareness for Taxpayers
Protect Your Clients; Protect Yourself
Tax Security 101

Subscribe to IRS Tax Tips