



## West Virginia Executive Branch

### Privacy Tip

IRS Tax Tip 2018-03, January 8, 2018

*The State Privacy Office occasionally offers tips for your "away from work" life. We hope these Tax Day tips from the IRS are beneficial to you.*

Taxpayers can follow a few simple steps to protect their personal and financial data online and at home. Criminals continue to steal large amounts of personal data from taxpayers and tax preparers. Thieves use that data to file fraudulent tax returns or commit other crimes while impersonating the victims.

All taxpayers should follow these steps to protect themselves and their data:

### Keep a Secure Computer

- Use security software that updates automatically. Essential tools for keeping a secure computer include a firewall, virus and malware protection, and file encryption for sensitive data.
- Treat personal information like cash; don't leave it lying around.
- Give personal information only over encrypted websites – look for "https" addresses.
- Use strong passwords and protect them.

### Avoid Phishing and Malware

- Don't respond to phishing emails, texts or calls that appear to be from the IRS, tax companies and other well-known businesses. Instead, verify contact information about a company or agency by going directly to their website.
- Be cautious of email attachments. Think twice before opening them.
- Download and install software only from known and trusted websites.
- Use a pop-up blocker.

### Protect Personal Information

- Don't routinely carry a Social Security card or other documents showing a Social Security number.
- Do not overshare personal information on social media. This includes information about past addresses, a new car, a new home and children.
- Keep old tax returns and tax records under lock and key.
- Safeguard electronic files by encrypting them.
- Shred tax documents before trashing.

People should also remember to watch out for IRS Impersonators. The IRS will not call someone with threats of jail or lawsuits. The IRS will not send an unsolicited email suggesting someone has a refund or that they need to update their account, the IRS will not request any sensitive information online. These are all scams.

Taxpayers should forward IRS-related scam emails to [phishing@irs.gov](mailto:phishing@irs.gov). They can report IRS-impersonation telephone calls at [www.tigta.gov](http://www.tigta.gov).

### More Information:

- [Identity Protection: Prevention, Detection and Victim Assistance](#)
- [Publication 4524](#), Security Awareness for Taxpayers
- [Taxes. Security. Together.](#)

Page Last Reviewed or Updated: 09-Jan-2018

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