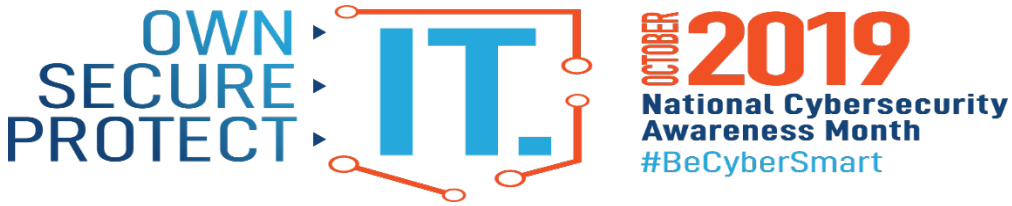
West Virginia Executive Branch
Privacy Tip



The first of the three key messages of NCSA Month is "Own IT", which is taking personal accountability for your online presence, and understanding your digital profile.

Simple Tips to Own IT:

- **Never Click and Tell: Staying safe on social media**
  - Limit what information you post on social media – from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to target you, your loved ones, and your physical belongings.
  - Remember – there is no delete button on the internet! Share with care. Just because you deleted a post or picture right after posting it, chances are someone still saw it.
  - Keep your connections on social media to people you know and trust.

- **Update Privacy Settings**
  - Set the privacy and security settings to your comfort level for information sharing. Disable geotagging, which allows anyone to see where you are – and where you aren't – at any given time.
  - To keep others from contacting people on your friend lists, make sure to set up the list for "only me" to see.

- **Keep Tabs on Your Apps: Best practices for device applications**
  - Change your device's factory default password immediately. Consider using the longest password or passphrase possible.
  - Properly secure your wireless network you use to connect to Internet-enabled devices. You may want to consider placing these devices on a separated and dedicated network. For more information, view the National Security Agency's Cybersecurity Information page.
  - ALWAYS update to the latest security software, web browser, and operating systems.

The Cybersecurity and Infrastructure Security Agency (CISA)
is part of the Department of Homeland Security
Reprinted with permission.

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