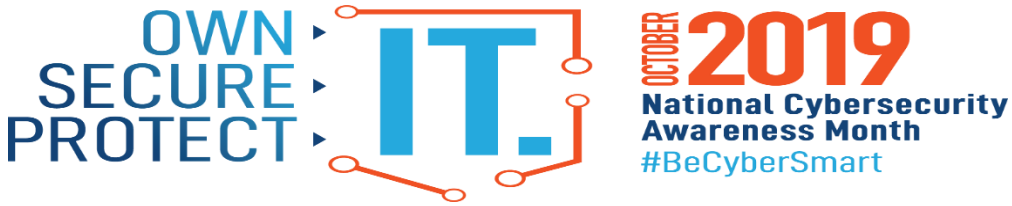
West Virginia Executive Branch
Privacy Tip



The second key message of NCSA Month is “Secure IT”, which is learning how to keep cyber-criminals from getting into your digital life.

Simple Tips to Secure IT:

- **Shake Up Your Passphrase Protocol**
  - Create strong, unique passphrases. This is one of the most important steps in protecting your devices. See Creating a Password for more ideas.
  - Consider using the longest password permissible for your devices.
  - Don’t use the same password for all of your accounts.

- **Double Your Login Protection: Turn on multi-factor authentication (MFA)**
  - Multifactor authentication (MFA) is defined as a security process that requires more than one method of authentication from independent sources to verify the user’s identity. The more methods that are required increase security.
  - MFA uses something you know (a password), something you have (a number sent to your mobile phone for verification), and/or something you are (your fingerprint).

- **Shop Safe Online**
  - Use familiar websites. There are many retailers that are here one day and gone the next. Or, research the site you want to purchase from. Read independent reviews (good and bad), and carefully read shipping and return policies.
  - Use a credit card, not a debit card. A hacker can clean out a debit account quickly.
  - Don’t use public wi-fi to shop. Security can be very spotty.

- **Play Hard to Get with Strangers: How to spot and avoid phish**
  - Beware of emails that look like a legitimate business, but the email address doesn’t reflect the business name at all.
  - Don’t click links in email. Hover over it to see if it matches the sender in any way.
  - A legitimate business will not ask for personal or financial information in an email.

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.