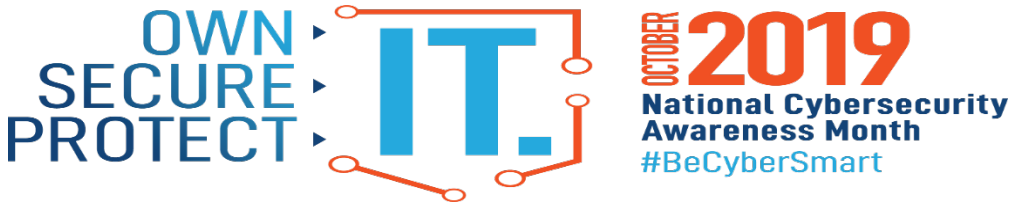
West Virginia Executive Branch
Privacy Tip



National Cybersecurity Awareness Month (NCSAM) – observed every October – was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online.
Since its original inception under leadership from the U.S. Department of Homeland Security and the National Cyber Security Alliance (NCSA), NCSAM has grown exponentially, reaching consumers, small and medium-sized businesses, corporations, educational institutions and young people across the nation. Now in its 16th year, NCSAM continues to build momentum and impact co-led by NCSA and the Cybersecurity and Infrastructure Agency (CISA).

NCSAM 2019 Theme and Key Messages
A New Direction
Following wide success of the 'Our Shared Responsibility' theme in years past, CISA and NCSA have shifted strategic focus to a message that promotes personal accountability. Driven through mass public engagement, the 'Own IT. Secure. IT. Protect IT.' theme will help to encourage personal accountability and proactive behavior in digital privacy, security best practices, common cyber threats and cybersecurity careers. Here is a breakdown of the highlighted calls to action and their key messages:

- **Own IT.**
  - Never Click and Tell: Staying safe on social media
  - Update Privacy Settings
  - Keep Tabs on Your Apps: Best practices for device applications
- **Secure IT.**
  - Shake Up Your Passphrase Protocol: Create strong, unique passphrases
  - Double Your Login Protection: Turn on multi-factor authentication
  - Shop Safe Online
  - Play Hard to Get with Strangers: How to spot and avoid phish
- **Protect IT.**
  - If You Connect, You Must Protect: Updating to the latest security software, web browser and operating systems
  - Stay Protected While Connected: Wi-Fi safety
  - If You Collect It, Protect It: Keeping customer/consumer data and information safe

Copyright © 2019 Stay Safe Online — NCSA. All rights reserved.
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.