



Welcome to National Cyber Security Awareness Month! All through October the Office of Information Technology will be sending out information about cyber security in an effort to raise your awareness of the risks of using the Internet. Each week, these posts will be announced via Twitter and Facebook as well as email, so be sure to follow @BerryCollegeOIT on Twitter and the BerryCollegeOIT page on Facebook. This week, October 3-7, focuses on the **STOP. THINK. CONNECT.** principles of online security.

STOP: make sure security measures are in place

Do you know how to recognize risks and potential problems? In case you miss something, is your anti-virus running and up to date?

THINK: about the consequences of your actions and behaviors online.

Is what you are about to do advisable? Could it reveal information about yourself you would not want others to know? Could it cause you or your reputation harm? Could it cause harm to someone else?

CONNECT: and enjoy the Internet.

After verifying your defenses and considering your actions, enjoy the Internet safely.

These three words involve the following concepts in practical terms:

- **Keep a clean machine**
 - Keep your computer up to date, especially your operating system and your anti-virus software
 - Protect all of your devices, not just your desktop or laptop, but your cell phones and tablets, too
 - Scan with your anti-virus software any and all portable storage devices you plug into your computer
- **Protect your personal information**
 - Turn on two-factor authentication on all your online accounts, if available, especially banking and shopping accounts
 - Use strong passwords at least 12 characters long
 - Use unique passwords for every account - a pain, but far more secure
 - Use a password manager to help you manage and remember all those passwords

- **Connect with care**
 - When in doubt, throw it out - links in emails and social media posts are many times cybercriminals trying to steal personal information
 - Don't conduct banking or financial transactions on public WiFi hotspots
 - Be sure any site where you conduct financial transactions is using "https" as the start of the address
- **Be web wise**
 - Think before you act - don't be fooled by emails that urge immediate action or offers that sound too good to be true
 - Back it up - back up your precious, priceless photos, videos, documents and other digital information to a separate hard drive, USB drive or cloud storage account.
- **Be a good online citizen**
 - Be careful what you post on social media - follow the Golden Rule - post about others as you would have them post about you
 - Help fight cybercrime - report any instances of stolen identity or finances immediately to the [Internet Crime Complaint Center](#)
- **Own Your Online Presence**
 - Protect your personal information, make sure apps and websites are not improperly gathering your information. Their privacy policy should be clear and easy to find.
 - Be aware of what you are sharing on social media. Set privacy and security settings to limit who can see your information
 - Be careful about what you post - consider what it reveals about you, who might see it, and how it might be perceived in the future

I hope you read and enjoy the weekly posts and that you can learn something new that will increase your cyber security awareness.