STOP | THINK | CONNECT™

Week 2: October 9th through October 13th

Cybersecurity in the Workplace Is Everyone's Business

Whatever your place of business is – whether it's a large or small organization, healthcare provider, academic institution or government agency – creating a culture of cybersecurity from the breakroom to the board room is essential and a shared responsibility among all employees.

Every organization needs a plan for employee education, training and awareness that emphasizes risk management, resistance and resilience.

Simple Tips

1. **When in doubt, throw it out.** Stop and think before you open attachments or click links in emails. Links in email, instant message, and online posts are often the way cybercriminals compromise your computer. If it looks suspicious, it's best to delete it.
2. **Back it up.** Make electronic and physical back-ups or copies of all your important work. Data can be lost in many ways including computer malfunctions, malware, theft, viruses, and accidental deletion.
3. **Guard your devices.** In order to prevent theft and unauthorized access, never leave your laptop or mobile device unattended in a public place and lock your devices when they are not in use.
4. **Secure your accounts.** Use passwords that are at least eight characters long and a mix of letters, numbers, and characters. Do not share any of your usernames or passwords with anyone. When available, turn on stronger authentication for an added layer of security, beyond the password.
5. **Report anything suspicious**. If you experience any unusual problems with your computer or device, report it to your IT Department.

Below are some links to helpful tips and information that can help keep you safe online:

- STOP.THINK.CONNECT. Basic Tips & Advice
- Privacy is good for business tip sheet
- Technology Checklist for Businesses
- Other Resource Documents

References:
- https://www.dhs.gov/about-stopthinkconnect
- https://staysafeonline.org/stop-think-connect