

April 2020 – Technology Security Tip

Cybersecurity Tips for Working Remotely During COVID-19

- **Use VPN when necessary.** Virtual private networks, which provide secure direct connections to your organization's computer network, might be necessary when accessing files, working with sensitive information or using certain websites. If you don't have VPN on your device, contact your company's help desk to see if it's available.
- **Update your router's software.** Home routers should be updated to the most current software and secured with a lengthy, unique passphrase.
- **Think before you click.** Avoid downloading or clicking on unknown links in emails. If you aren't sure if you should, call the sender first. Hackers often use fake websites to trick you into giving sensitive information or to install malware onto your device. [Get more tips.](#)
- **Guard your devices.** If your organization allows you to work elsewhere from your home, never leave your laptop, tablet or cellphone – including any USB or external storage devices – unattended. Avoid entering passwords where others can see.
- **Create strong passwords.** Be sure they include a mix of upper and lowercase letters, numbers and symbols. Make them difficult enough that someone can't guess them.
- **Don't share passwords online.** If you must share log-in information with a coworker, call them with the details instead of sending via email, text or instant message.
- **Use two-factor authentication.** Although it can be inconvenient, two-factor authentication, if available, provides an extra layer of security to keep hackers from accessing accounts.
- **Encrypt your email.** Some data and information might need to be encrypted before sending it electronically. This might also include information that you might otherwise share in a conversation if you were at the office.
- **Update your devices.** If you are using a personal device that's been approved for teleworking, be sure that it's running the most current operating system and that your web browsers and other applications are also up to date. Also be sure you are running an up-to-date and modern anti-virus software solution. Updates include important changes that improve the performance and security of your devices.

Courtesy of NC DIT