west protect℠

SAFE Tipsheet

Security Tips for Working from Home

May 2020

As more businesses and employees work from home, basic security measures need to be taken to protect the individual and enterprise from cyber criminals who are taking advantage of lax telework security practices. So here are some tips, some familiar and some new that may help you stay in top shape and avoid the consequences of weak security practices.

Basics (you should already be doing):

Think Before You Click. Now cyber criminals are taking advantage of people seeking information on COVID-19. They are distributing malware campaigns that impersonate organizations like WHO, CDC, and other reputable sources by asking you to click on links or download outbreak maps. Slow Down. Don't Click. Go directly to a reputable website to access the content.

Lock Down Your Login. Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device to identify that you are really you!

New Basics of Working from Home:

Connect to a Secure Network and use a company-issued Virtual Private Network (VPN) to access any work accounts. Home routers should be updated to the most current software and secured with a lengthy, unique passphrase. Employees should not be connecting to public WiFi to access work accounts unless using a VPN. If you don't have a company-issued VPN, you should look for a personal one to use to provide the same protections.

continued on next page

SAFE Tipsheet

Security Tips for Working from Home

continued from previous page

Separate your network so your company or work devices are on their own WiFi network, and your personal non-work devices are on their own network.

Keep devices with you at all times or stored in a secure location when not in use. Be sure to lock your computer when you step away. You can also set auto log-out if you walk away from your computer and forget to log out.

Limit access to the device you use for work. Only the approved user should use the device (family and friends should not use a work-issued or your work-only device).

Use company-approved/vetted devices and applications to collaborate and complete your tasks. Don't substitute your unapproved tools with ones that have been vetted and approved for use by the company's security team. If you don't have company-approved devices and applications, be sure to look into each one and choose the best one to use securely, and learn how to set the security and privacy setting.

Update your software. Before connecting to your corporate network, be sure that all internet-connected devices - including PCs, smartphones and tablets - are running the most current versions of software. Updates include important changes that improve the performance and security of your devices.

Regardless of where you are, the National Cyber Security Alliance urges all internet users to stay safer and more secure online by updating software on all devices (including antivirus and firewalls) backing up data, enabling multi-factor authentication and having strong, lengthy passphrases for each online account.