SURGICAL INFORMATION SYSTEMS™

INFORMATION SECURITY

SECURITY TIPS FOR REMOTE WORKERS

As we are all adjusting to working from home, basic security measures need to be taken to protect both ourselves and the company from cybercriminals who are taking advantage of the reduced level of security on our home networks. To help better protect yourself and SIS, please follow these tips provided by the National Cybersecurity Alliance.

Think Before You Click

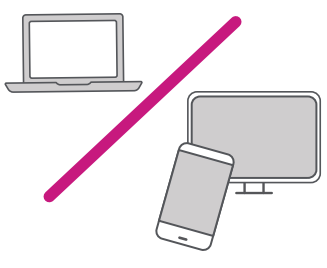
Cybercriminals are taking advantage of people seeking information on COVID-19. They are distributing malware campaigns that impersonate organizations like WHO, CDC, and other reputable sources by asking you to click on links or download outbreak maps. Slow down. Don't click. Go directly to a legitimate website to access the content. DO NOT provide your credentials or open attachments from any email you are not expecting.

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.

Connect To A Secure Network 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 from their corporate-issued device.



Separate Your Network

Keep your company devices on their own WIFI network, and your personal devices are on their own. In this hyperconnected age, our home networks often have a large number of smart devices connected, such as TVs, games consoles, refrigerators, etc. These devices quite often have little to no security and can be used to gain access to your home network. Segregating these devices from the corporate device can significantly reduce the possibility of a security incident.

Keep Devices With You At All Times Or Stored In A Secure Location When Not In Use

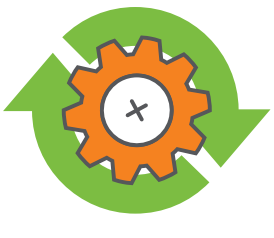
Set auto log-out if you walk away from your computer and forget to log out.

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 device).

Use Company-approved/vetted Devices And Applications

Use only approved tools that have been vetted by the company's security and IT teams. Do not substitute those with personal or preferred tools when collaborating or completing your tasks.



Update Your Software

The IT team automates the installation of the latest security updates released by Microsoft to your corporate laptop. If you are prompted to reboot your system, please do so as soon as possible. A reboot is often required to complete the installation process and ensure your system is secure. For all other devices such as phones, tablets, and other network-connected devices, ensure they all are up to date with the manufactures latest security releases to protect both yourself and the company further.

SEC_RITY IS NOT COMPLETE WITHOUT "U"