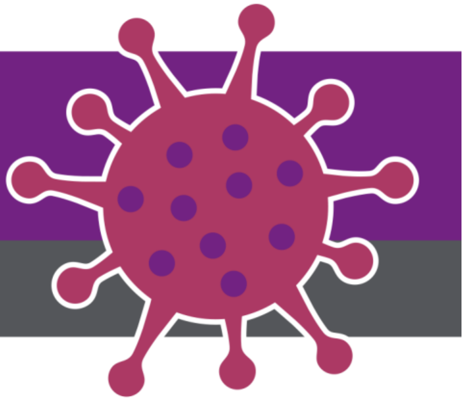
CORONA**VI**RUS **D**ISEASE 2019
(COVID-19)

Protect Your Personal Devices, Your Home and Our Network From Cyber-Attacks



Trinity Health

Audience: All Colleagues	
Revision Date: 4/15/2020	
Version: Version #1	

Protect Your Personal Devices, Your Home and Our Network From Cyber-Attacks

Among the many challenges we are all now faced with, attacks by cybercriminals have increased tremendously. There has never been a more critical time to protect your home, personal devices and our network, from cyber-attacks involving malware and viruses. Below are some helpful security measures that all of us should take, especially colleagues accessing the Trinity Health network with their personal devices.

Secure your personal devices (PCs, laptops, tablets, phones)

- **Install reputable antivirus and malware software.** It may be available from your Internet Service Provider (ISP) for free. Scan your devices for malware and viruses regularly. Make it a habit.
- **Update your device Operating System (OS) software and stay current.** These updates frequently provide patches to protect your device and information from recently known cyberthreats.
- **Use network firewalls.** Firewalls are a frontline defense to prevent cybercriminals from accessing your devices and information.
- **Back up your important personal information** offline to an external hard drive or in the cloud. You may be really glad you did this at some point.
- **Set strong passwords.** Consider using a password manager application.
- **Enable multi-factor authentication (MFA) for your key accounts,** like banking apps and peer-to-peer payment apps. This added layer of security hinders thieves from tampering with your financial accounts.
- **Use device encryption** to make your personal information nearly impossible to crack.
- **Turn your devices off when not in use.** Cybercriminals have a tough time doing something with systems that are turned off. This also creates a reboot which may assist antivirus software to attack malware.

Secure your home router

- **Update router software regularly.** Like your devices, these software updates frequently provide patches for the latest protection needed.
- **Update the manufacturer default name and password if you're still using them.** This information is often known and used by cybercriminals.
- **Set a strong password on your router.** Everything that cybercriminals might attack needs a complex password.
- **Turn off remote access management.** This hinders unwanted access to your router configurations from anywhere in the world.
- **Lock down Wi-Fi access.** Set the Security level to WPA2.

Note that securely setting your router can vary slightly by manufacturer. Consider doing a web search that includes your router manufacturer name. You'll immediately have a tailored list of the exact, easy steps to follow.

For other Information Security questions or requests email **Ask Cybersecurity**.