# Security In The Remote Work World—CoronaVirus Edition

## Corona Virus Scams Abound!

Scammers are targeting consumers using phishing, phony websites, and even telephone and door-to-door scams. Be cautious! *Always* validate the credibility that phone calls, websites and email sources are legitimate. A significant number of "coronavirus" and "COVID-19" domains have been registered in recent days, often appearing to be from the Centers for Disease Control and Prevention (CDC), but really owned by dangerous spammers. Researchers have already found malware that was spread via the legitimate-looking email address CDC-Covid19@cdc[.]gov.

***If you receive an email or text claiming to have news about coronavirus, do not open it!***

Find timely, accurate updates at these reliable sources: https://coronavirus.delaware.gov/, https://cdc.gov **OR** https://www.who.int/

— ***Solomon Adote,*** Chief Security Officer

The current epidemic has introduced many new people to remote work. While working at home the bad guys can try to use you as a backdoor into your state, K12 or company work. It is important to take the following precautions while working at home.

## Secure Your Home WI-FI

**Change the name of your router from the default.** The name of your router (or SSID) is likely to be a default ID assigned by the manufacturer. Change the name to something unique that only you know.

**Change your router's pre-set password(s).** Your wireless router's manufacturer assigned a standard default password that allows you to set up and operate the router, as its "administrator." Hackers know these default passwords, so change it to something only you know. Visit the company's website to learn how to change the password.

**Turn off any "Remote Management" features. Always remember to log out as Administrator.** Once you've set up your router, log out as administrator to lessen the risk that someone can piggyback on your session to gain control of your device.

**Keep your router up-to-date:** To be secure and effective, the software that comes with your router needs occasional updates. Before you set up a new router and periodically thereafter, visit the manufacturer's website to see if there's a new version of the software available for download. To make sure you hear about the latest version, register your router. with the manufacturer and sign up to get updates.

## Secure Your Home Computer

**System and Software Updates -** Ensure the automatic system update feature for your specific Operating System is turned on.

**WINDOWS USERS** Go to the Start button, then Settings, Update & Security, Windows Update, and select Automatic Updates. Enable other application software, such as browsers and MSOffice software to automatically update. For Windows users, only use Windows 10 or newer supported Operating Systems (Windows 7 is end-of-life).

**MAC USERS**: Click on the Apple, top left, then About this Mac, then click Software Update button, and assure you have checked the box, Automatically keep my Mac up to date.

**Anti-Malware -** Validate you are running an UpToDate anti-malware/anti-virus solution on your home computer. Most newer windows computers have windows defender built in. Ensure it is running and fully updated.

**Internet Service Providers (ISP)** offer free anti-virus to their customers.

| COMCAST | VERIZON |
|---|---|
| Xfinity | FIOS |

An alternative source for anti-virus is included below:

Windows MAC OSX Chrome

**MAC/OSX**: Some other useful tips to validate anti-malware (XProtect) protection and other built-in security features are turned on: https://mashtips.com/built-in-mac-security-software/.

## Protecting Your Organization's Information

Coordinate with your organization's Information Security Officer regarding the specific requirements surrounding remote and/or virtual access to the data necessary to work from home. Remember:

✓ If your organization offers Remote Desktop Protocol (RDP) to an office computer, try to keep the confidential data on the office computer while you work on it. Bad guys can use your personal computer to steal your organizations data if not secured. Your office computer is always better secured for the office data.

✓ Never disclose confidential or sensitive data to any unauthorized personnel including friends and family.

✓ Do not store sensitive or confidential information on your personal computer. Store any sensitive or confidential information on encrypted media provided by your department. Better yet, do not move or copy such information off your work computer.

✓ Always lock your computer when leaving it unattended.

*Questions, comments or topic suggestions?* Email us at eSecurity@delaware.gov