Cyber Security & COVID-19

Title Agent Security

The current COVID-19 situation has caused many Members to send employees home to continue supporting your operations and your customers.

Adjusting to work-from-home conditions and the stress of the pandemic makes it the perfect time to discuss protecting you and your company from a security incident. We are recommending you implement or confirm your basic security hygiene and at-home security protection.

Basic security hygiene is the foundation to protect yourself, your company, and your customers.

Unique passwords – Utilize unique passwords for each website, application, or service you access with a username and password. This helps ensure if a password is compromised the risk is contained to one website, application or service and not all.

Strong passwords – Having a unique password is not enough; the password you choose should be strong and include at least 8 characters (14 or more is better), lowercase, uppercase, number 0 – 9, and a special symbol.

Change passwords on a periodic basis – The recommendation is to change your password at least every 90 days.

Use a password manager – A password manager can be used to store and secure all of your passwords for all of your applications to enable you to be able to have a unique password for every service.

Use multi-factor authentication – Using multifactor authentication for all high-risk applications and services adds a strong layer of defense to ensure applications and services do not experience unauthorized access. Multifactor authentication is the method in which a person is allowed access to applications and services based on an authentication that includes **(a)** something you know, **(b)** something you have, or **(c)** something you are.

(Continued on back)

In the case of logging into an application you have something you know (Username and password), something you have (two factor token), or something you are (fingerprint or face recognition). This is important especially for email and production applications.

Use reputable U.S. based antivirus software – Run antivirus/malware protection on computers and mobile devices that is provided by an U.S. based security company.

Use firewall on computers – Always have your firewall enabled on your computer even if you are on a trusted network.

Limit physical access to computers – All computers should be locked when not in use and lock should be set to automatically occur if idle for 15 minutes or less.

Secure laptops and mobile devices – Don't leave laptops or mobile devices unsecured at any location to include in back seats of cars or in a car trunk.

Email Security – Only use reputable email providers and use multifactor authentication to access your email account.

Sensitive data sharing – When sharing sensitive data avoid email and use a secure transfer method to ensure data is protected.

Avoid public Wi-Fi connections – Public Wi-Fi connections are not secure and sensitive data can be intercepted if you are not careful. If you must use public Wi-Fi, ensure you are connecting to a Virtual Private Network (VPN) while on the public Wi-Fi. To be secure just avoid public Wi-Fi all together.

Mobile Apps – Only official app stores for mobile devices should be used to purchase or download apps. Also, when using a mobile app ensure you are only giving rights to the mobile app that are really needed. An example would be that a flashlight app has no reason to access your contact list or your photos.

Charging equipment – There are ways to steal data and take over your mobile devices through charging equipment. Only use your own charging equipment when charging your mobile devices and skip the cables offered by ride share, airports, or other public charging options.

With the shift of the workforce, at-home security protection is critical to protect yourself, our company, and your customers.

Clean desk – When working at home you may have physical data that should be cleaned off your desk and locked away when not in use. Data should never be left out for others to see so a clean desk is important.

Secure equipment – Ensure that equipment taken home is secured physically to avoid theft from visitors and service providers. Lock equipment away when not in use.

Secure your network – When possible use an ethernet cable connection at home; however, if you do utilize wireless access point ensure your wireless is utilizing the WPA2 security protocol.

Implement a Guest Wi-Fi access point – If possible, use work computers on the standard Wi-Fi access point and have guests, family and household utilize a Guest Wi-Fi access point to segment your business from non-business.

Digital assistants – Voice command digital assistants have added convenience to our everyday lives; however, they are listening to every word within hearing range. You will want to turn off digital assistance when having confidential or conversations that exchange sensitive data to avoid the information from being recorded.

Guests and Family Members – When working from home you may have guests or family members in the home. They should not be allowed to use work computers.

It's a turbulent time for most of us as we deal with the current world situation. Practicing good security hygiene and at home security protections can protect you, your company and your customers from security incidents.

For more information visit:
thefund.com/cybersecurity