SECURE YOUR HOME OFFICE

MIND THE GAP CYBER

> “Rogue actors want it. You need to guard it. Data is worth more than gold in today's digital age.”

The COVID-19 pandemic in the spring has forced many businesses to move to remote work. The trend continues as many states are pausing their plans due to an uptick in new cases and companies that can have their employees to stay home.

As you continue to work from home, you must review what measures you have to be cyber secure. Remember to carve out a dedicated workspace for yourself and try to keep your desktop or laptop your work-only, especially if you are work for a company using your own devices.

Here are actions you can do right now to make your home office more secure:

Create Hard Passwords

Most use the same password everywhere and share a password with family or coworkers. Hackers know that is the weakest link. Password managers create and save unique, highly complex passwords automatically and fill them in at sites you want to log in at—based on one strong master password or key.

Some of the best-known password managers:
LastPass

Dashlane

1Password

In the macOS Mojave and iOS 12, Apple has provided a password manager free of charge.

At the least, use 2-factor authentication for every vital website and service you use, i.e., banking, insurance, and social media platforms.

Check Your Router Settings

You have a WiFi router in your home, providing internet access to family and friends. It is one of the weak links in your home office security chain. If you are concerned about the security of files over WiFi, use a VPN (see page 3) and hardware your connection directly to the router via a cable.

Set a complicated router password is the first thing you can do. A WiFi password needs to be 12 or 20 characters long. If it is painful to remember, then it is a secure password. Remember to change your password regularly.

Limit access to your WiFi network to those living in the house. Vendors or salespeople don't need access to your WiFi.

Once you have created a strong WiFi router password, you need to change your router's admin credentials. I bet you never thought of doing that, but all devices come with factory-installed user and password. So if you know the password, the bad guys do too.

After changing the admin credentials, change the network name or SSID name to something bland, then hide your network and strengthen WiFi encryption to WPA2 AES. Most newer routers have this option.

Like with your computer, routers have firewalls. Turn on your computer and router firewalls.

SECURE YOUR HOME OFFICE

MIND THE GAP CYBER

> “Rogue actors want it. You need to guard it. Data is worth more than gold in today's digital age.”

Use A VPN

A virtual private network or VPN is a connection method used to add security and privacy to private and public networks. A VPN protects your data on the web by using advanced encryption protocols and secure tunneling techniques to encapsulate all online data transfers.

There are many VPN providers out there. Go with a paid provider. If you are a small business, these VPNs providers suggested by TechRepublic are respectable, allow for multiple connects for your team, and work on PC/Mac.

Prices varied from $40.00/year to $80/year. Well worth the investment to keep data secure.

Express VPN

SurfShark

CyberGhost

IPVanish

Private Internet Access

Norton VPN

SECURE YOUR HOME OFFICE

MIND THE GAP CYBER

> “Rogue actors want it. You need to guard it. Data is worth more than gold in today's digital age.”

Install and Update Antivirus Protection

Antivirus/malware software is a crucial component of any Windows, Mac, or mobile operating system, especially workstations that access the internet and are used for financial transactions or access and store confidential data.

While there are free services, pay the money for paid. Most of the paid services have auto-update and scanning options in the settings. Prices and services vary, so pick one that meets your needs. Many offer trials.

There are many providers on the market, TechRepublic lists some of the more established:

Norton Antivirus

McAfee Total Protection

Symantec Endpoint Protection

Kaspersky Endpoint Protection

Malwarebytes Cybersecurity

Microsoft Defender

Disclaimer: *Use your judgment when selecting any software or hardware. I am not affiliated with any of the providers listed, nor do I receive any compensation.*

Have more questions?

Contact Ann Marie van den Hurk, APR, Founder
+1 401.217.9594 o • +1 302.563.0992 m • Ann@MindTheGapCyber.com

www.MindTheGapCyber.com