Coronavirus Home Office Security –

Practical Tips for Securing Your "New" Home Office

I've been working as an independent consultant for quite some time. Along the journey, I've picked up many tips and tricks to maximize productivity while working from home with great results. There have been many articles written about this issue and I hope to add some serious security ideas to the discussion that you may not have considered.

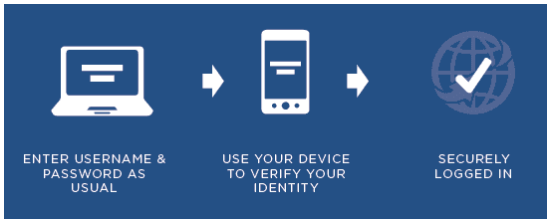
Many of you are being told to work from home with no idea on where to start and what matters the most. This article is going to focus on practical information to help you secure your home office. Check with your company to see if there are any protocols in place. If not, start with these basics.

Use strong passwords and a password manager

Passwords should be unique for every account and should comprise a long string of upper- and lower-case letters, numbers, and special characters. Clearly, it's difficult to remember all these passwords, which is why password managers are such popular tools these days. I use LastPass for saving and accessing passwords but of course there are other products available I particularly like LastPass because anything you save to LastPass on one device is instantly available to you on any other device you use. if you don't already have a LastPass account, you can get started by signing up for a free trial at **https://lastpass.com/create-account.php.** I am not affiliated with LastPass in any way.

Set up two-factor authentication

Multifactor Authentication is an added layer of security that you can enable within LastPass and requires a second step before you can gain access to your account. Enabling this security feature helps protect your account from



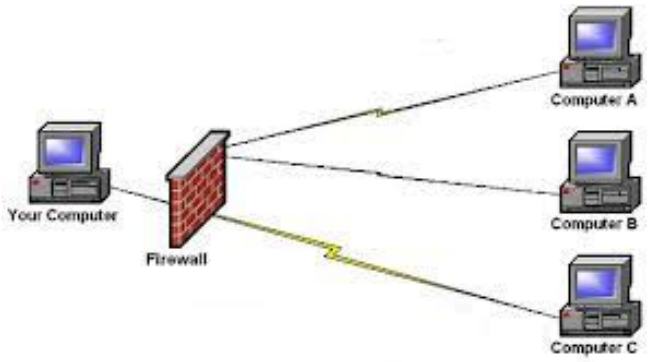
keyloggers and other threats – even if your Master Password was compromised, your account could not be accessed without this second form of authentication.

Use a VPN

A Virtual Private Network, or **VPN,** is a piece of software that changes your IP address and encrypts all of your internet traffic. This improves online privacy, security, and helps users to bypass online censorship imposed by the government, ISPs or any other organization or person blocking websites. A popular main reason to use a VPN is to protect your online information and to visit websites that can be hard to enjoy locally. When left unprotected, your private data, such as bank account information and credit card numbers, can fall into the wrong hands. A good VPN encrypts your data, so even if you connect to a public wi-fi network, your private data is guaranteed to be protected.

Set up firewalls

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.



Your home internet provider may already have a firewall in place so check before your bother to set one up

Use an antivirus software

Antivirus software is nearly as crucial as a PC's operating system. Even if you're aware of potential threats and practice extreme caution, some threats just can't be prevented without the extra help of an AV program—or a full antivirus suite.

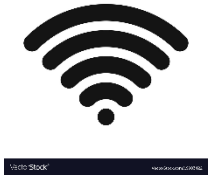
Antivirus software is critical for EVERY PC or device you use at home. Without it, you risk losing your personal information, your files, and even the cash from your bank account.

AV software can keep your Windows PC safe from spyware, Trojans, malware, and more.

There are quite a few great choices out there for you can easily find with a Google search, or better yet, ask your IT person what he/she recommends.

Secure your home router

Wireless internet or Wi-Fi access has become a necessity in the home and workplace, but it can also open a door to risks from hackers, scammers, and identity thieves. Whether in your home or office, an unsecured Wi-Fi router running on the default manufacturer settings could be a liability when it comes to hackers and Wi-Fi squatters accessing your private information and burdening your broadband.



If your Wi-Fi network isn't secured properly — a public IP address, no unique Wi-Fi password — you could be letting anyone with a wireless-enabled device to gain access. You might not be worried about someone using your wireless connection, but the real risk is exposing sensitive information you send and receive — your emails, banking information, and maybe even your smart home's daily schedule — to cybercriminals.

Install updates regularly

Microsoft Update is the online extension of Windows that helps you keep your computer current. Microsoft Update includes updates from Windows Update and from Office Update, in addition to updates for other Microsoft products and for third-party device drivers. Use Microsoft Update to install updates for your computer's operating system, software, and hardware.

New content is added to the site regularly so that you can obtain recent updates and fixes to help protect your computer and to keep it running smoothly. To use the Microsoft Update site to install all critical updates for your computer, follow these **steps**.

I choose the other route: automatic updates. By using Automatic Updates, I don't have to visit the Microsoft Update Web site to scan for updates. Instead, Windows automatically delivers them to my computer and installs them automatically.

Back up your data

The main reason for data backup is to save important files if a system crash or hard drive failure occurs. There should be additional data backups if the original backups result in data corruption or hard drive failure.

Additional backups are necessary if natural or man-made disasters occur.

Encrypt your hard drives in Windows 10

Simply locking your PC with a password isn't enough, as hackers can still find ways to bypass the lock screen. Windows Hello makes the processes a lot harder considering it relies on biometrics, but in cases where your information is stored on a secondary hard drive that can be pulled out, biometrics become largely irrelevant.

The good news is that you can still protect your information on Windows 8 by using BitLocker drive encryption.

In both cases you need the Pro version of Windows, not Home.

BitLocker can be used to secure both internal and external hard drives. It doesn't only function after signing into Windows, it can also determine if a security threat is present during the boot up process, so you're fully covered.

MacOS has encryption built in regardless of the version.

Beware remote desktop tools

Remote desktop tools aren't new but with organizations becoming increasingly international and teams becoming more mobile they're fast becoming essential.

A search for remote desktop software reveals a myriad of options. It can be overwhelming navigating past rogue tools, confusing interfaces, and buggy services.

For a great overview, take a look at the **10 Best Free Remote Desktop Tools**.

Look out for phishing emails and sites

What is phishing? Phishing is a cybercrime in which a target is contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. Don't buy into these schemes.

The FTC has a great **article** surrounding phishing. Take the time to educate yourself on this very real threat.

The FBI's IC3 (Internet Crime Complaint Center) has a chart showing the huge amount of loss victims have been taken for. What's extremely sad is how the scams focus so much on our elderly.

2019 VICTIMS BY AGE GROUP

Victims		
Age Range[6]	Total Count	Total Loss
Under 20	10,724	$421,169,232
20 - 29	44,496	$174,673,470
30 - 39	52,820	$332,208,189
40 - 49	51,864	$529,231,267
50 - 59	50,608	$589,624,844
Over 60	68,013	$835,164,766

Use encrypted communications

In the legal profession, encrypted communications could be critical since we're dealing with attorney client privilege so often. I used the website **https://haveibeenpwned.com/** and checked my email to see if I had been a victim of a breach and sure enough, I have two out of three emails that have been breached. There are several tools to stop this from happening to you (I installed one myself) and you can find a great list at **https://www.techradar.com/best/best-encryption-software** including free, paid and business tools and services.

Check your bar association to see if encryption is required in your state to protect confidentiality.

Lock your device

To lock your computer:

Press the Win+L key combination on the computer keyboard (Win is the Windows key).

Windows key features the Windows logo.

Click the padlock button in the lower-right corner of the Start button menu. Clicking the padlock icon locks your PC. Why lock your computer? I know you didn't ask that question, right? For step by step directions, go to **https://www.wikihow.com/Lock-a-Computer**.

Hopefully, I set out some helpful information and tips for you to assist the transition to your new unfamiliar environment. Working from home can certainly have its benefits, but it also comes with major responsibilities. Take the time to implement those responsibilities.

Gayle O'Connor, Independent Marketing Consultant, **gayle@gmomarketing.com** 3/24/2020