How to Protect Yourself Working from Home

1) **BROWSERS:** Keep your Browser, Operating System and Virus software up to date. Check for updates on a daily base because new threats hit the web daily.! Windows and Mac put out releases frequently when bugs and zero-day exploits are found. Zero-Day exploits are major bugs found in software and reported to the software manufacture for patch fixes.

   In addition, adjust web browser security settings. For example, disable (or limit) cookies, create and configure trusted zones, turn on phishing filters, restrict unwanted websites, turn on automatic website checking, disable scripting (such as JavaScript and ActiveX), and have the browser clear all cache on exit. All of these things can help to filter out fraudulent online requests for usernames, passwords, and credit card information, which is also known as web-page spoofing. Higher security settings can also help to fend off session hijacking, which is the act of taking control of a user session after obtaining or generating an authentication ID.

   Moreover, if a window pops-up and wants you to enter a password or something else Don't click OK or Agree to Close a Window; instead press Alt+F4 on the keyboard to close that window, or use the Task Manager and click "End Task."

   Here is a list of some of the most dangerous viruses for 2020
   https://www.safetydetectives.com/blog/most-dangerous-new-malware-and-security-threats/

2) **Firewall's:** Have your Firewall enabled and running; It will prevent others from seeing you online and it will prevent hackers from getting into your system. To open Windows Firewall. Click Windows Icon "Win+ R" Type: firewall.cpl
   On a Mac click System Preferences then Security and Privacy. Click turn-on Firewall

3) **PORTS:** Common Ports on your computer you need to either disable or protected from outside hackers. What is a Port? - Port 80 is the standard port used by your web browser to communicate over the web, and port 143 is your standard IMAP used for email. In addition, Windows system's files and Print Sharing protocols on port 137-139 is used by NetBIOS. If you don't want a hacker to connect to these shared ports which the entire internet can also see disable/block them or filter them using your firewall. Some of the more common ports: like FTP: port 21, SSH: Port 22, Telnet: 23, HTTP: 80

and HTTPS: 443 are critical ports that should also be closed or monitored with your firewall setting.

If you want to really see what is happening on your network and who might be connecting to your computer. Use **Netstat** in the Command line. Windows Icon "Win+R" then type **cmd**. In Mac the command-line is a program called Terminal.

Netstat is a command line tool for monitoring network connections both incoming and outgoing. **Netstat** is available on all **Unix-like Operating Systems** and **Windows OS**. It is one of the most basic network services debugging tools, telling you what ports are open and whether any programs are listening on ports. Run Windows Command-Line tool or Mac's Terminal and type in these commands.

Listing all ports (both TCP and UDP) using **netstat** -a option.
Type: netstat -a | more
Listing only **UDP** (**User Datagram Protocol**) port connections using **netstat -au**.
Type: netstat -au
Listing all active listening ports connections with **netstat -l**.
Type: netstat –l

4) **ROUTERS**: Routers use all the ports listed above and many others. One-way hackers get into your router is by the Domain Name Server (DNS) Poisoning.

Illustrated Guide to the Kaminsky DNS Vulnerability.
http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

DNS poisoning and DNS spoofing are also known as resolution attacks. DNS poisoning occurs when an attacker alters the Domain-Name-to-IP-Address mappings in a DNS system to redirect traffic to a rogue websites or systems, or to simply perform a denial-of-service against a system.

When the DNS server is poisoned to carry out a pharming attack the records have been changed so that instead of sending the correct IP addressing to you. It sends you IP to a fake web site created by the attacker collecting everything you input. This has been done to Banking web site getting you to login to a fake Bank Portal and stealing your User Name and Passwords.

Another popular means of performing a man-in-the-middle attack is through DNS cache poisoning. Similar to **Address Resolution Protocol** (ARP) cache, once a client receives a response from the DNS, that response will be cached for future use. If false information can be fed into the cache, then misdirecting communications is trivially easy. In simpler terms an ARP attack is a technique by which an attacker intercepts communication between network devices and now is receiving any data that is intended

for the users IP address. “Think of it as a party line the hacker can listen in on.” There are many means of performing DNS cache poisoning, including HOSTS poisoning, authorized DNS server attacks, caching DNS server attacks, DNS lookup address changing, and DNS query spoofing

DNS poisoning focuses on sending an alternate IP address to the client to be used as the DNS server the client uses for resolving queries. The DNS server address is typically distributed to clients through DHCP but it can also be assigned statically. Even if all of the other elements of IP configuration have been assigned by DHCP, a local alteration can easily assign a DNS server address. Attacks to alter a client’s DNS server lookup address can be performed through a script (similar to the ARP attack mentioned earlier) or by compromising DHCP. Once the client has the wrong DNS server, they will be sending their queries to a hacker-controlled DNS server, which will respond with poisoned results

To see DNS setting on your router are normal type: http://whoismydns.com/
Check to see if your DNS server correlates with your Internet Service Provider.
Also check your routers setting are normal click the link below.
https://www.grc.com/x/ne.dll?bh0bkyd2

5) **WHO IS ON MY SYSTEM?** In Windows you have Task manager which is a tool you can use to see if someone has remoted into your system. Right click on the task bar and click **Task Manager**. Once its running just Click the Users Tab. In Mac it’s called the **Activity Monitor**. To launch the Activity Monitor on your **Mac**. You can find it in the /Applications/Utilities folder. Under the Process Name list, select the app or process you want to quit. A better way is to download Windows SysInternals or Mac’s Powertoys.

The SysInternal tool is like Task Manager on Steroids. It lets you do all types of thing the Task Manager does not do, and it’s a great tool to find bugs and virus on your system. It would take too long to go into all things it does, just download it and watch a YouTube video. “ITS GREAT….!” The tool is free and you can download it from Microsoft web site. https://docs.microsoft.com/en-us/sysinternals/downloads/

The Mac OS has a similar tool called “Powertoys.” Here is one link for **“Powertoys,”**
https://github.com/microsoft/PowerToys/releases/

6) **Browser Add-Ons:** Browser add-ons can be great tools for changing fonts, adding search options, managing passwords to encrypting data. They can also harbor viruses so know what your downloading and who it is coming from. In addition, delete any add-ons you no longer need or want.

In Chrome: Installed Chrome extension
"C:\Users\[login_name]\AppData\Local\Google\Users"
Data\Default\Extensions" folder. Each extension is stored in its own folder named after the ID of the extension.
Or click on the 3 dots in the right-hand corner of your browser, go too more tools and Extensions. If you want to add a new extension:

- Open the Chrome Web store
- Find and select the extension you want
- Click Add to Chrome
- Some extensions may need certain permissions or data and make sure only approve extensions that are trusted.

In Firefox: Click on the Three-Bar menu button in the upper right corner and click Add-ons. Scroll through the list of extensions and click the three-dot icon next to the extensions you want to remove. Select Remove to delete, or Manage to review details or permissions.

In Safari on a Mac: Choose Safari > Preferences, Click Extensions. Here you can turn on/off the Extension or choose to "Uninstall." To add an Extension, click Safari > Safari Extensions, then browse the available extensions. The best Extensions will let you manage and customize it to your personal preference. If you need more help, "How to install Safari extensions on your Mac." https://support.apple.com/en-us/HT203051

Extension's Safety Tips for any Browser; Be wary of the permissions you grant to any extension. A lot of extensions are created by third-party developers. So do your research before you install an extension that might have hidden functions. Here are a few rules to follow before you click install.!

- Is the extension created by a brand name or trusted developer?
- Check the developer's website, blog, or social media for information?
- Has the extension been installed by others on the web and does it have a good star rating?
- Do the permissions it is requesting match with the features of the extension? Example: Is it requesting location information, access to your email contract list? If these requests do-not make sense or explain why they need this information, **DO NOT CLICK YES.!**
- The Firefox Add-Ons Website may have more information about the extension: https://addons.mozilla.org/
- To view a list of extensions officially endorsed by Mozilla https://support.mozilla.org/en-US/kb/permission-request-messages-firefox-extensions

- Safari for Mac: Here is a list of some of the better extensions for your Mac. In addition, click the view button to read more about the app and its features. Also take a look at its star rating. https://apps.apple.com/us/story/id1377753262
- Finally: Read the Privacy Policy and understand the information it is collecting about you and what it will do with that information.

7) **Hid your Wi-Fi foot-print from hacker eyes**:

Your router is broadcasting – **HERE I AM, HACK ME**.! Your router has a name and it's called **Service Set Identifier** (SSID) is used as an identifier to distinguish one access point from another. You can think of it as something similar to a domain name for wireless networks. To hid it, log into your router with your IP address, and if you don't know it here is how to find it.

In Windows open a command window – "Windows Icon "Win + R" and type **cmd** in the command-line, and then type "**ipconfig**." Look for the Default Gateway, the number for example will look something like this: 192.68.0.1. Now just open a browser and type that into the Query String aka search bar.

In a Mac you would open a Terminal and navigate to /Applications/Utilities; press enter or just type Network Utility into Spotlight to open it then type "**ifconfig**." This command with no arguments will display all the active interfaces details. A quicker way for MAC is to just type in "**netstat -rn |grep default**" This is your network router. Now just input that into a browser search bar and look for the setting of the SSID. There are many types of routers on the market and each one is a little different, but search for the SSID broadcasting options, by default its most likely enabled, switch it to off.

Remember write down you SSID name before disabling it or you may get locked out of your network.

Useful Commands to Protect your System	
1) Netplwiz	Hidden tool in Windows gives you control over the user account. Open up the Command-line and type this in: netplwiz
What this does is it requires you to press Ctrl+Alt+Delete before signing in. This guarantees that the authentic Windows sign-in screen that appears, is not one created by a hacker thus protecting the system from programs that mimic a sign-in to retrieve and steal password information. Check the Box: **Require users to press Ctrl+Alt+Delete**	
2) ipconfig/flushdns	Clears DNS Cache type this within the Command-line
To ensure Windows is getting addresses from the new DNS servers instead of using old, cached entries, run the **ipconfig /flushdns** in the command-line.	
3) Sudo killall -HUP mDNSResponder - this is the Mac command to flush DNS.	

In Mac it depends on the OS version, but try the command this way. Run terminal.app and launch Applications -> Utilities or press Command + Space. Type in the command above and hit return.	
4) Tracert	Example: tracert www.google.com In command-line
Tracert command, which traces the route it takes for a packet to reach a destination.	
5) Eventvwr.msc	View all events on your Windows system
Win+R, then type eventvwr.msc – view all errors and events happening on your system. In Mac it's the Console app.	
6) Problem Steps Recorder (psr.exe).	In Windows if you have a problem and need to contact IT support.
Problem Steps Recorder will record the step-by-step interactions that occur while the user replicates the problem, taking screenshots of every action. Good tool to run if you have a problem and want to show it to someone.	
7) Ping	In the Command-line type Ping www.address.com for example
Ping is a *command*-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable	
8) Hosts File Modifications	Defense against DNS Poisoning:
Modify the computer's hosts file permissions to read-only. It is located at the following path: **%systemroot%\System32\drivers\etc**	
For more information visit: https://en.wikipedia.org/wiki/Hosts	
9) Netstat ?	To see a list of other useful netstat commands
Displays a full list of protocol statistics and current TCP/IP network connections	
10)Msconfig	To run type "win + R" type in command
Once open click the Tools Tab for a list of Services and Operations you can launch.	

8) **Viruses: Is my computer infected with a virus. Here are some typical symptoms of viruses:**

- Computer runs slower than usual.
- Computer locks up frequently or stops responding altogether.
- Computer restarts on its own or crashes frequently.
- Hard drives, optical drive, and applications are not accessible or don't work properly.
- Strange sounds occur.
- You receive unusual error messages.
- Display or print distortion occurs.
- New icons appear or old icons (and applications) disappear.
- There is a double extension on a file attached to an e-mail that was opened; for example: .txt.vbs or .txt.exe.

- Antivirus programs will not run or can't be installed.
- Files have been corrupted or folders are created automatically.
- System Restore capabilities are removed or disabled.

9) **Virtual Box: it's an in-memory sandbox that does not affect your main operating system.**

If you want to truly be safe from viruses and hackers install a VirtualBox on your computer. Then install any browser, software or operating system you use to surf the web. Oracle VM VirtualBox is one of the best, but there are many others and most like Oracles are free to download and use. If the software app gets infected just delete it and install a new version in the VirtualBox. It wipes it out of memory and does not affect your main operating system at all – ITS VIRTUAL.!

It's very easy to install and YouTube has many videos on how to install it. Here are a few links to help you get started.

VMware Workstation Player
https://www.vmware.com/products/workstation-player.html

Windows Virtual PC
https://www.microsoft.com/en-us/download/details.aspx?id=3702

QEMU
https://www.qemu.org/download/#windows

Parallels
https://www.parallels.com/products/desktop/

XenServer
https://www.techjunkie.com/best-virtualbox-alternatives/

Oracle VM VirtualBox
https://www.oracle.com/virtualization/technologies/vm/downloads/virtualbox-downloads.html

I tried to cover as much as I can without being too technical.

Play safe, work hard and virus free.