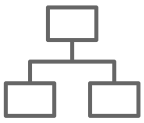
18 THINGS to Make Your Remote Work **Secure, Convenient, and Stress-Free**

New to remote work? There are a lot of processes IT has put in place to make your lives easier and more secure in the office. If you're transitioning to work from home, our ***Eggspert*** checklist can help you put similar processes in place to make your experience more secure, reliable, and, ultimately, more enjoyable. For more information, see our detailed summaries.

- ☐  Take a picture of your computer setup before you unplug and take things to your remote work location—including the cable setup in the back!
- ☐  Install updates.
- ☐  Update antivirus and anti-malware tools, too.
- ☐  Uninstall unnecessary software from your personal computer.
- ☐  Use the virtual private network (VPN) at all times.
- ☐  Turn off automatic connections on your Wi-Fi.
- ☐  Separate your network.
- ☐  Lock your computer.
- ☐  Create a different user account for family and/or friends.
- ☐  Use a password manager.
- ☐  Ask your IT person about securing the DNS settings on your personal computer.
- ☐  Update your softphone software.
- ☐  Ensure secure browser configuration.
- ☐  Use Mozilla® Firefox® or Google® Chrome™ as your browser.
- ☐  Think twice.
- ☐  Don't be click happy.
- ☐  When in doubt: See something, say something, ASAP.
- ☐  **Check with your IT team to make sure your data is being backed up!**

Ready to Learn More
Check out the details below.

1) Take a picture of your computer setup before you unplug and take things to your remote work location—including the cable setup in the back!

At home, your IT team won't be with you to reconnect everything. A quick picture of where things are plugged and arranged may save you hours of frustration later. And don't forget to use an approved cleaning agent to wipe things down before you disconnect.

2) Install updates.

Particularly if you're working from a computer you already own but don't typically use for office work, please check that all updates and patches to Microsoft®, Adobe®, and other critical software applications have been installed. We know, updates take time, and it's all-too-convenient to click 'Remind Me Later.' However, many vulnerabilities exist in out-of-date software and are the perfect entry-point for a hacker. You must protect the data that you are entrusted to access. Keep it safe by ensuring your software is up to date.

3) Update antivirus and anti-malware tools, too.

As a follow up to number two, this may sound obvious. These tools are highly valuable and are designed to reduce risk and keep your computer safe from threat actors that want access to your company's data. However, just like your office tools, it's easy to postpone those time-consuming updates—ultimately leaving you at risk. If you're using a home computer for your work and do not have a paid-for antivirus and anti-malware solution, ask your IT team for help installing a licensed, approved corporate security software to use while working remotely.

4) Uninstall unnecessary software from your personal computer.

If you are using a personal computer, please uninstall software that isn't being used by your family. Software that isn't being used usually isn't being updated or patched. Those patches prevent hackers from entering through known vulnerabilities. By removing unwanted or unused programs, you have reduced that risk.

5) Use the virtual private network (VPN) at all times.

We understand that it's just one more thing that you need to do before you can work. Think of it as your seatbelt when you get in the car to drive. That extra moment it takes could be the moment that saved your office network from an attack. And don't forget to re-engage the VPN every time you log on. It's easy to put your computer to sleep when you walk away to grab lunch, forgetting that you' ve logged off the VPN.

6) Turn off automatic connections on your Wi-Fi.

One easy way for hackers to gain access to your computer is Wi-Fi spoofing. For example, let's say you routinely connect to 'Joe's Wi-Fi,' so much that to save time, you click the button that says, 'Connect Automatically.' A hacker can set up a portal called 'Joe's Wi-Fi,' and your computer may unwittingly connect automatically to that portal because it has been identified as a safe network.

7) Separate your network.

When possible, connect your computer to a different network than the rest of your remote location. It may be as simple as using the company VPN to create that secure connection. If you are more technically capable, then separate your company computer from the rest of the computers in your remote work location via a different router or firewall. If your mobile data plan allows for unlimited data, consider using the hot spot on your phone instead of a guest network or your home network.

8) Lock your computer.

When you aren't using your computer, just like at the office, lock the computer to keep family, friends, and maybe even the kids next door from accessing your company data. And while you are thinking about computer use, please remember that your company computer is for business use only. While it might be convenient to check the news or order takeout, please limit personal use and do not allow friends and family to use your work computer. Something as simple as a local

restaurant's takeout menu could end up being a malicious file that exposes your computer to malware.

9) Create a different user account for family and/or friends.

If you plan to use your personal computer for remote work, create a separate user profile for you that is different than your other family members or friends. This is a major step towards helping the company meet our cybersecurity objectives.

10) Use a password manager.

If your company offers a password manager, please don't forget to use it to create and store passwords. The goal is to avoid saving passwords in the browser that can be easily swiped. We know sometimes it's easier to save it in the form or use the same passwords for different sites or forego using multi-factor authentication where it is offered. However, sacrificing the convenience is well worth it to avoid a security incident and loss of data. Oh, and remember that using a spreadsheet to save your passwords isn't much better than saving them in the browser forms. Avoid that when you can.

11) Ask your IT person about securing the DNS settings on your personal computer.

They likely have the software or a tool you can use on your home computer that will help keep you from accidentally going to the wrong places.

12) Update your softphone software.

If set up correctly, softphones, like voice over IP (VoIP), can be very convenient. However, if they are not secure, they can be exploited fairly easily by cybercriminals. If you are using a softphone system at home, make sure you are taking active preventative measures to avoid hacking.

13) Ensure secure browser configuration.

Google Chrome extensions can be a hotbed for computer viruses. It's best not to use them at all. However, at the very least, make sure those you are not using are uninstalled. If you're not sure how to do this, ask your IT professional.

14) Use Mozilla Firefox or Google Chrome as your browser.

Many other browsers can contain vulnerabilities that can open you up to a variety of cyberattacks, ultimately leaving company data exposed. Both Mozilla Firefox and Google Chrome have the most up-to-date security.

15) Think twice.

The threat actors, also known as cybercriminals, are looking to take advantage of you when you least expect it. Right now, receiving an email that looks like it came from your boss or CEO with a subject line that reads, "Company Coronavirus Update" may seem normal, but it may not actually be from your company. Take a moment to review who it came from (the actual email address, not the name in the display). Also, question whether this person would typically send you an email like this.

16) Don't be click happy.

Just because there is a link or an attachment does not mean that you need to click. Mouse over the link and see where it wants to take you. Check for the actual spelling of the domain in the area before the .com, .net, .edu, .gov, or .org looking for anything unusual like the characters '1', 'l,' or 'I' being leveraged as an imposter domain. Another example would be the letters 'rn' instead of 'm' or 'vv' instead of 'w.'

17) When in doubt: See something, say something, ASAP.

You are our firewall, the first line of defense against threat actors trying to invade our network. And while we know you will never click on a fake email, in the event anything odd seems to have happened, we'd rather know about it than ignore it and hope it goes away. If you may have done something that afterward, seemed suspicious, let us know as soon as possible. And if you accidentally did something that later you realized was bad, disconnect your computer from the VPN and network and call us right away.

18) Check with your IT team to make sure your data is being backed up!

Have questions? Need some help?

Contact a friendly Eggspert today!

www.EggHeadIT.com | **(760) 205-0105**

