18 TIPS To Make Remote Working **Painless** and **Protected**

IT has put in place many processes to make your lives streamlined and more secure in the office. If you're working from home for the first time, this checklist can help you put similar processes in place to make your experience painless and protect your set up.

- ☐  Snap a pic of your computer setup before you unplug and bring things to your home office. Don't forget the cable set up in the back!
- ☐  Install updates.
- ☐  Update your antivirus and anti-malware tools.
- ☐  Remove unnecessary software from your personal computer.
- ☐  Stay connected to 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 guest 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!**

Want to Learn More?
Read 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 there to reconnect everything. A picture of where things are plugged and arranged can save you from frustration later. And remember to use an approved cleaner to wipe things down before you leave the office.

2) Install updates.

If you're working from a computer you already own but don't usually use for office work, check that all updates and patches to Microsoft®, Adobe®, and other important software has been installed. We know, updates take time, and it's convenient to click 'Remind Me Later.' However, many vulnerabilities exist in out-of-date software and are an easy entry-point for a hacker. You must protect the data that you access. Please keep it safe by ensuring your software is up to date.

3) Update antivirus and anti-malware tools.

This may sound obvious. These tools are valuable and built to reduce risk and keep your device protected from bad guys that want to access your company's data. However, just like your office tools, it's easy to delay those time-consuming updates—ultimately leaving you at risk. If you're using a personal computer for work and do not have a paid-for antivirus and anti-malware solution, ask your IT team for help installing a licensed, approved enterprise security software to use while working remotely.

4) Remove unnecessary software from your personal computer.

If you're using a personal computer, uninstall software that isn't being used by your family. Software that isn't in use 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) Stay connected to the virtual private network (VPN) at all times.

We know that it's just one more thing that you need to do before you can work. But think of it as your seatbelt when you get in your car to drive. That extra second it takes could be the moment that saved your office network from an attack. Remember to re-engage the VPN every time you log on. It's all too easy to put your computer to sleep when you walk away to grab a coffee, forgetting that you've logged off the VPN.

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

An easy way hackers gain access to your computer is Wi-Fi spoofing. For example, say you frequently connect to 'Starbucks 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.

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

8) Lock your computer.

When you aren't using your computer, just like at the office, lock the computer to keep unwanted users -family, friends, kids- from accessing your company data. Please remember that your company computer is for business use only. While it might be convenient to check the news or order takeout, try to 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 guest account for family and/or friends.

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

10) Use a password manager.

If your company offers a password manager, remember to use it to create and store passwords. The goal is to evade saving passwords in the browser that can be easily wiped. We know it's easier to save it in the form or use the same passwords for different sites and skip using multi-factor authentication where it's available. However, sacrificing the convenience is completely worth it to avoid a security incident and loss of data. 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 a software or a tool you can use on your home computer that will help keep you from going to the wrong places.

12) Update your softphone software.

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

13) Ensure secure browser configuration.

Chrome extensions can be a breeding ground 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 browsers can contain vulnerabilities that can expose you 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.

Threat actors are looking to take advantage of you when you least expect it. Getting an email that looks like it came from your boss with a subject line that reads, "Company Coronavirus Update" may seem normal, but it may not actually be from your company. Take time to review who it came from (the actual email address, not the name in the display). Ask if 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. Hover 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 the first line of defense against threat actors trying to invade your network. And while we know you would never click on a fake email, in the event anything odd seems to have happened, we want to know about it rather than ignore it and hope it goes away. If you may have done something that afterward, seemed suspicious, let IT 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 IT right away.

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

TWINSTATE TECHNOLOGIES®