PLATTE RIVER NETWORKS
PEOPLE · PASSION · PARTNERSHIPS

15 THINGS TO MAKE YOUR REMOTE WORK SAFER AND EASIER

1. Install updates

Please check that all updates and patches to Microsoft®, Adobe®, and other critical software applications have been installed.

2. Update antivirus and anti-malware tools

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.

3. 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.

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

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.

5. Turn off automatic connections on your Wi-Fi

One easy way for hackers to gain access to your computer is Wi-Fi spoofing; including your neighbors if you are sharing. If your mobile data plan allows for unlimited data, consider using the hot spot on your phone instead your home network.

6. Lock your computer

When you aren't using your computer, just like at the office, lock the computer to keep anyone else from accessing your company data. Please remember that if you brought home a company computer, it is for business use only. 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.

7. 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.

8. Use a password manager

The goal is to avoid saving passwords in the browser that can be easily swiped. Platte River Networks recommends using our Single Sign On solution. Please call 303-255-1941 for more information.

PLATTE RIVER NETWORKS
PEOPLE · PASSION · PARTNERSHIPS

9. Use Mozilla Firefox or Google Chrome as your browser and ensure secure browser configuration

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. Keep in mind, 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 Platte River Networks 303-255-1941.

10. Think twice

Right now, receiving an email that came from your boss or CEO with the subject line, "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) and question whether this person would typically send you an email like this.

11. Be aware of fake COVID-19 Emails, links, attachments, etc.

Do not open emails regarding COVID-19 from unknown senders. These could be phishing scams. Do not click on links in emails regarding COVID-19. Do not download or open email attachments from unknown senders. These could contain viruses and other malware.

12. Be careful

Exercise caution when providing personal information. Be very suspicious of requests for personal information that occur via email, phone, text message, or social media message.

13. 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.'

14. When in doubt: See something, say something, ASAP

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 303-255-1941

15. Slow computer?

If experiencing slowness ask who in the house is streaming music, videos, etc. Also, if you have a data drop outlet available then plug your computer into your home network versus wireless.

FOR QUESTIONS OR MORE INFORMATION PLEASE CONTACT PLATTE RIVER NETWORKS AT 303-255-1941

Thank you ConnectWise, Webroot and the Platte River Networks team for contributing their expertise and input to this list.