I’ll have a Vanilla Caramel Latte and that hacker over there will have all of my company’s information.

Working remotely in a coffee shop or outside on a sunny day – it sounds perfect right? You’re able to get your work done, but also enjoy your favorite latte or take in some fresh air and sunshine at the same time! Thanks to the abundance of hotspots and free WiFi connections available these days, it easy to work from almost anywhere. Yet by working through a public WiFi connection, are you putting your information (as well as your company’s information) at risk?

Many companies invest substantial assets in order to provide employees with access to computers to perform the responsibilities of their jobs. Employees who are provided with computers or access to computers in the course of their jobs have significant responsibilities regarding their use. Here are some precautions to help keep that information secure especially when working remotely:

Make good use of your firewall

Always start with the basics. Be sure that your mobile firewall is on. Most operating systems have a basic firewall pre-installed, but it may not be something that is automatically enabled. Check to see that it is on and operating to give yourself at least another layer of protection when accessing public Wi-Fi networks.

Ensure the site you are using is encrypted

Sites that encrypt their data make it unreadable to others, which is important for pages that require you to plug in passwords, social security numbers, account numbers, and other confidential information. Many websites that ask for confidential data automatically take this step for you, yet it makes sense to check for yourself to ensure you’re not handing over sensitive information across a public connection. Look for URLs that start with https:// rather than just http:// for the most secure connection. For employees who are required to work many hours away from the office, many companies provide a VPN, or Virtual Private Network for them to use. A VPN offers the security of a private network when you’re using an unsecured public WiFi connection. All of the information sent or received will be automatically encrypted.

Refuse to share

Sharing is good, right? Not on public WiFi it isn’t. When working remotely, be sure to check your file and print share options so that you’re not leaving your data out in the open. Since this option enables file-sharing between more than one computer or printer, your private data (or your company’s private data) may be more easily accessed when sharing is left on, especially if it’s not password-protected. This is one of those situations when refusing to share is actually a good thing. Check to make sure your data sharing options are disabled and you have a good chance of KEEPING your private information private.

Do you really need to connect?

It’s almost automatic when using a public network to log on, and then just stay connected for the duration of your visit. If you only need to access a certain amount of information online, and can then log off and continue to work offline, be sure to do so. You limit your exposure to hackers the less time you spend actually connected. It’s also a good idea to double-check the name of the Wi-Fi connection before logging in. Sometimes similar-sounding networks are created by hackers to collect passwords and other information, so be sure the one you are logging into is actually the one you want. Usually you will be asked for a password, which also helps ensure security.

Look over your shoulder

It goes without saying that you should always be aware of those around you and to never leave sensitive data or information lying around. If possible, do your banking or expenses at home. Pay your bills somewhere else. Don’t enter your credit card info or account numbers over a public WiFi connection if you don’t really need to.

Employees must remember to exercise their best judgment and common sense at all times when working remotely. However, if you feel that any Company secure information has been compromised while you are working remotely, do not try to cover up the problem. In this case honesty is the best policy. Be sure to inform your Company as soon as the breach is known.

For additional information or specifics on how to best protect your company’s data while working remotely, contact McCloskey Partners today! We have years of proven experience helping small businesses like yours understand the complexities of their human resources needs and decisions.

McCloskey Partners, LLC 623 W. Market Street, Perkasie, PA 18944; 215-453-1978 phone; 215-220-3422 fax; www.mccloskeypartners.com; email info@mccloskeypartners.com.

Find us on Facebook, Pinterest, Twitter and LinkedIn: McCloskey Partners.