Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

COVID-19 Security TIPS when Working from Home

March 23, 2020 – Many employees are now forced to work from home, which may be a new experience for them. Cyber security risks are increased when people are faced with unfamiliar circumstances. Here are some tips to help make the working from home experience as secure as possible.

Whenever possible use a company-owned computer, NOT your personal computer, to work from home. The company computer should have the necessary anti-virus and encryption software to ensure the data is protected. Also, company I.T. staff will be familiar with company devices and therefore be better able to help answer questions and resolve issues.

- If you have WiFi in your home, make sure that you have encryption turned ON (this will require you to enter a password before you connect) and that the password is long (24 characters) and not easy to guess. This will help prevent neighbors or others accessing your network and intercepting work-related information.
- DO NOT let your children or other family members play with or use your company computer for any reason. Restrict YOUR use of the computer to business purposes only. This will reduce the possibility of downloading something malicious onto the computer.
- If you have limited Internet bandwidth in your home, you may experience slow computer response, or some functions may not work correctly. Limit the bandwidth used by other devices during working hours (TV, audio steaming, etc.) and if you are meeting with others via Skype, Zoom, GoToMeeting, etc. limit the meeting to AUDIO only, as video webcams use more bandwidth.
- Use a Virtual Private Network (VPN) to connect to the office. This will protect data that is transferred back and forth from being intercepted.
- DO NOT save files or documents on your local computer, put them where they belong on the home network (Shared disk, etc.) Otherwise, working remotely could end up meaning files are scattered and inaccessible to others.

For more information, please contact William Prohn at wprohn@dopkins.com.