CYBERSECURITY

Work securely from home

Our homes have become our workplaces. How do we protect our systems and our data from being compromised when we work outside the office, in particular from our homes?

As cybercriminals quickly adapt to large portions of the global workforce working remotely, homes and the technology employees use have become prime targets. There are also particular risks to business data that arise when employees are all working in different home environments.

Cybersecurity is a partnership. Your business may have invested in technology designed to secure systems and data. While this is a significant step in protecting against potential cyberattacks, your employees play a critical role as the first line of defence.

Below are five steps employees can take to secure their home office and help prevent data loss.

Five steps to securing your home office

Secure your home network

- Change the default administrator name and password on your network router and Wi-Fi devices and make sure they are running the latest manufacturer updates. Employees can call their internet provider to get instructions on how to do this. This step is key, as hackers know the default network names and passwords for most providers.
- Require a strong password to join your Wi-Fi network and use the latest encryption (WPA2).

- Review the devices that connect to your network (e.g., phones, gaming consoles, lights, TVs or even your car) and disconnect those that aren't necessary. Make sure those that remain use strong passwords.
- Use a separate "guest" wireless network for your friends.
- If possible, do not "broadcast" your wireless network name (SSID). Employees can contact their internet provider to determine how to change that setting.

Contact your service provider or equipment manufacturer for additional support – quite often, service manuals for the equipment are online.

Secure your computers and devices

- Don't use your work computer for unnecessary personal tasks.
- Keep your work computer in a secure location and lock it (typically WIN-L or Ctrl-Alt-Delete and click lock) before leaving it unattended.
- Don't allow family or friends to use your work computer or any other company-issued device.

Secure your personal accounts and passwords

- Use strong passwords that are hard to guess and even passphrases where possible (e.g., "Where Is My Coffee?").
- Use different passwords for each of your internet accounts, services and devices.
- Never repeat passwords between company systems and your personal services and devices.
- Change passwords frequently.

Secure your personal information

- On social media, post only what you want the public to see, and think about the permanent information you may be unwittingly sharing about yourself or your family.
- Don't fall victim to cyberscams (click here for more information on this topic).

Secure and control what you print

- Only print what you need to do your job; wherever possible, avoid printing sensitive commercial or personal information.
- Don't forward company data to personal email, even if just to print; company data should always remain on company devices.
- Any material you print that relates to work could be found by someone and compromised if you don't dispose of it properly. Unless the material you print from your work computer is public information, shred it at home or store it in a box for later secure disposal.

Visit us at victorinsurance.ca to learn more.