MicroAge®

A QUICK GUIDE TO

Staying Secure When Working Remotely

Table of Contents

INTRODUCTION

As the world learns to adapt to the changes brought about by a global pandemic, identified as COVID-19, many businesses have asked their people to work remotely so they can continue to support and service their customers. For many of these businesses and employees, working remotely is a new and unknown work environment.

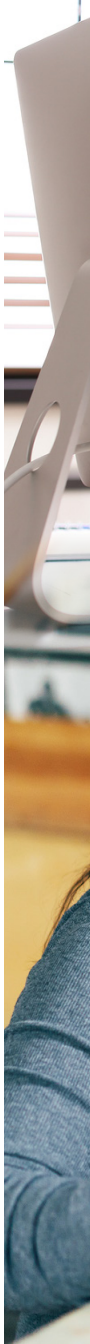
For cybercriminals, this means opportunity. They are using the concerns and uncertainty brought about by the virus to prey on people for whom working remotely is new. Simultaneously, there is evidence from the Canadian Centre for Cyber Security to show that bad actors are using concerns of the virus to prey on those same people. It is more important than ever that employees understand their role in protecting their personal data and their company's data.

From how employees work, to home networks, to what family members are doing online, every part of an employee's remote work life plays an important and critical role in ensuring the future of business continuity.

This quick guide provides some best practices and guidance to help businesses and their people work from home safely and securely.

REMOTE WORKERS:

1. Report any suspicious activity to your IT service provider or internal IT team.
2. Remain cautious and vigilant when reading emails, messages, web browsing, and be aware of phishing techniques. Many attacks have been launched using COVID-19 content as the delivery mechanism for malware. Here is a cheat sheet on how to recognize phishing emails.
3. Avoid non-reputable websites or links that may be potentially malicious.
4. Avoid public networks (i.e. coffee shop WiFi) and stay on your home network.
5. Make sure your home WiFi is secured, ideally with WPA2 or WPA3 protected access. Ensure insecure features like Universal Plug and Play (UPnP) are disabled. Although these features are convenient, you are trading convenience for security. Also ensure that default logins to IoT devices are changed.
6. Work within cloud applications where possible to make sure data is being backed up.
7. Protect you and your family's personal accounts with Two-factor or Multi-factor authentication, staying vigilant with interactions on online platforms.
8. Use strong passwords and ideally a Password Manager which store and manage passwords.
9. The more devices in use (phones, game consoles, etc.), the slower your connection which can hamper your ability to work remotely. Try to limit your family's bandwidth usage.



Employees using Personal Laptops and Desktops

- Ensure you have a reputable Antivirus and Firewall installed and turned on. Check with your internet service provider (ISP) to see if they provide free security suites.
- Ensure the latest operating system and web browser updates are installed.
- Lock your personal computer when walking away from it (Win+L on Windows or Command+Control+Q on Mac).
- Avoid the use of file sharing (P2P or peer to peer), and other high risk applications.

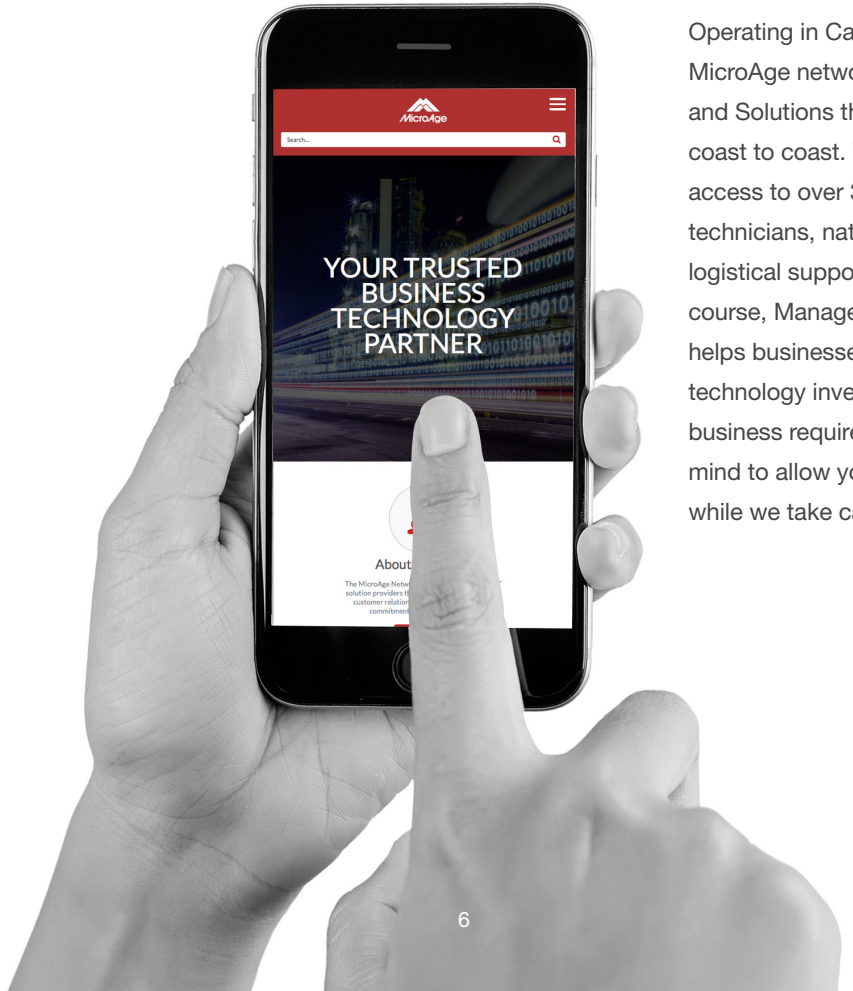
What not to do

- Use unsupported methods of communication to conduct business (We recommend using Teams)
- Use unsupported 3rd party VPN software/services
- Reuse passwords across personal and company accounts
- Store company proprietary information/work on personal devices
- Leave your business accounts logged in on shared system(s)
- Use your personal email(s)/accounts to conduct company business
- Connect unknown devices (USB sticks, peripherals, etc.) to company system(s)
- Install software that may put your system(s) at risk (Unsupported remote desktop, etc.)
- Wait to report any adverse information or suspicious activity identified with company assets

Conclusion

We are all having to quickly adapt to the new business realities. Providing best practices and guidance on how to stay secure when working remotely helps protect the business and it's people from those that are actively trying to take advantage of a situation that is already difficult on many levels.

About MicroAge



Operating in Canada since 1981, the MicroAge network delivers IT Services and Solutions through 37 locations from coast to coast. We provide businesses with access to over 300 knowledgeable, certified technicians, national service delivery, logistical support and distribution, and of course, Managed IT Services. MicroAge helps businesses of all sizes leverage their technology investments to address their business requirements. We offer peace of mind to allow you to focus on your business while we take care of your IT.


Contact **MicroAge** to learn more about working remotely securely.
MicroAge
www.microage.ca