Tips to Make Remote Work Secure, Convenient and Stress Free

Technology is one of the most important, yet most overlooked aspects of working from home. We like to think our digital world is plug and play and infinitely portable, but there are a few set-up and security measures you need to be mindful of to make your home office and related technology as functional and resilient as possible.

Getting started and using your workstation

Install updates

If you're using your own personal computer, make sure to install all updates and patches to Microsoft®, Adobe® and other critical software applications. Many security vulnerabilities exist in out-of-date software and could compromise your employer's sensitive data.

Install and update antivirus / anti-malware software

If you're using your own personal computer and do not have paid antivirus / anti-malware installed, request a corporate license from your IT department. If you already have a solution installed, make sure it's running the most recent updates and patches.

Uninstall unnecessary software

If you're using your own personal computer, uninstall any software that you or your family is no longer using. Old applications may not have been updated or patched recently and could pose a significant security risk.

Turn off automatic WiFi connections

Automatic connections are like candy for a WiFi spoofing cyber criminal. All they have to do is set up a fake malicious network to look just like yours and wait for your computer to take the bait. Make it harder for them by setting all your devices to manual.

Separate your network

When possible, connect your computer to a different network than the rest of your remote working location. Your organization's VPN is a great start, but using a different router or firewall is even better.

Secure the domain name system (DNS) settings on your personal computer

If you're using your own personal computer, IT will likely have software or a tool you can use to help secure your DNS settings and prevent cyber criminals from re-directing you to malicious websites.

Install / use Google Chrome for internet browsing

Chrome is the most reliable browser currently available and offers the latest and most up-to-date security.

Secure your browser configurations

Avoid using browser extensions wherever possible. At the very least, uninstall extensions you're not currently using.

Update softphone software

Voice over IP (VoIP) and other softphone services can be extremely functional and convenient, but they're also easy for hackers to exploit if they're not running current software and patches.

Always use the virtual private network (VPN)

A VPN does more than connect you to your organization's internal network — it also connects your computer to your organization's extensive security controls and makes it exponentially harder for cyber criminals to see, let alone breach your computer.

Create a separate work-only account

If you're using your own personal computer, use a different login for work than for personal or friends and family use. This helps to secure sensitive information and can reduce your employer's exposure to potential data breach.

Only use your work computer for work

Limit personal use as much as possible and do not let family or friends use your work computer. Websites are crawling with malware and there's too much sensitive information on your device to risk someone else's carelessness causing a security breach.

Lock your computer

Just like at the office, always lock the computer whenever you step away from your desk. It's easy to become lenient with this in a place as seemingly secure as your home, but hackers are counting on you to let your guard down.

Use a password manager

Store all your login information on a company-supplied or otherwise highly reputable password manager. Avoid re-using the same password for multiple sites and applications. Do not save passwords on websites or in the browser. And use multi-factor authentication wherever possible.

Back up your workstation every day

Your organization may do this automatically — but check in with your IT department for their best practices and recommendations to ensure consistent and reliable backups.

Be wary of topical emails

Your boss or CEO may very well be sending an all staff Weekly Coronavirus Update — but cyber criminals are counting on your complacency. Double check the email address, name and sender's signature to ensure the correct spelling and conventions of your organization.

Spotting suspicious activity

Watch where you click

Mouse over links or attachments in incoming email and see where they wish to take you before you click on them. Check the domain name spelling — look for characters like '1', instead of 'l', 'rn' instead of 'm' or 'vv' instead of 'w.

See something? Say something right away.

Contact your IT team about anything you feel is suspicious. They would rather have 100 false alarms than one successful breach.

About MNP

MNP is a leading national accounting, tax and business consulting firm in Canada. We proudly serve and respond to the needs of our clients in the public, private and not-for-profit sectors. Through partner-led engagements, we provide a collaborative, cost-effective approach to doing business and personalized strategies to help organizations succeed across the country and around the world.

For more information contact, Kerry Mann,
National Leader of Enterprise Resource Planning at
647.480.8400 or kerry.mann@mnp.ca