CYBER SECURITY TIPS FOR REMOTE WORK

APRIL 2020

ITSAP.10.116

When you work in the office, you benefit from the security measures that your organization has in place to protect its networks, systems, devices, and information from cyber threats. Working remotely provides flexibility and convenience. However, remote work can weaken your organization's security efforts and put you at risk if you don't take precautions. Read through our cyber security tips to ensure that you are practicing good cyber hygiene when working from home, a café, or any other public location.

MOBILE DEVICES

Without a dedicated workstation, you rely on mobile devices (e.g. smart phones, laptops, tablets) when working remotely. If possible, work only from corporate devices assigned to you by your employer.

- **Use multi-factor authentication.** You can add an additional layer of security to your devices by changing your settings to require two different factors to unlock it. For example, use a password or PIN **AND** a biometric, such as your fingerprint.
- **Keep your devices in sight.** Don't leave them unattended when you're working in a public location and report a lost or stolen device immediately to your IT help desk.
- **Check your surroundings.** Be aware of anyone who might be listening to your phone call or looking over your shoulder as you enter your password.
- **Run updates and patches on your devices**. Updates and patches address and fix security vulnerabilities, ensuring that your device is protected against threat actors.
- **Enable firewalls and anti-virus software**. Firewalls block malicious traffic and anti-virus software scans files for malware.

WI-FI

When working from your home, you should take steps to protect your own Wi-Fi network. Be sure to change the default password that was given to you by your service provider, and make sure that you are using a passphrase or a strong password that is difficult to guess.

The benefit of working remotely is that you can switch up your working location. Whether you are working at home, a library, or a café, you should always use a secure wireless network. Avoid sending sensitive information, whether it's personal or work-related, over a public Wi-Fi network. Using a virtual private network (VPN) is another way to protect information. A VPN is a secure encrypted tunnel through which information is sent.

PHISHING SCAMS AND SOCIAL ENGINEERING

Scammers steal sensitive information by pretending to be someone they're not. They may even use information from your social media accounts to make it seem like they know you — a tactic called social engineering.

- **Be vigilant**. Take care when you receive messages or calls from someone you don't know and requests that come out of nowhere.
- **Trust your gut**. If a phone call or a message is threatening or sounds too good to be true, it probably is.
- **Think twice**. Check a link's URL by hovering your cursor over it and don't open unexpected attachments.
- **Err on the side of caution.** Avoid sending sensitive information over email or texts.

LEARN MORE

These tips are a great place to start, but you can read through some of these related publications to find out more:

- *ITSAP.00.100 Spotting Malicious Emails*
- *ITSAP.00.266 Instant Messaging*
- *ITSAP.10.096 How Updates Secure Your Devices*
- *ITSAP.30.032 Best Practices for Passphrases and Passwords*
- *ITSAP.80.101 Virtual Private Networks*

All of these publications (and more) are available on the Canadian Centre for Cyber Security's website: **cyber.gc.ca**.

AWARENESS SERIES