Cyber security tips for remote work

CANADIAN CENTRE FOR CYBER SECURITY

March 2024 | 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 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, such as smart phones, laptops, and tablets, when working remotely. If possible, work only from corporate devices assigned to you by your employer. If you are not supplied with a corporate device contact your organization for guidance on corporately approved products. Unsecured endpoints can pose a risk to your organization's data and network.

Use multi-factor authentication: You can add an additional layer of security to your devices by changing your settings to require 2 different factors to unlock it. For example, use a password or PIN and a biometric, such as your fingerprint. To learn more about MFA, see Secure your accounts and devices with multi-factor authentication (ITSAP.30.030).

Keep your devices in sight. Don't leave them unattended when you're working in a public location. Report a lost or stolen device, whether corporately owned or personal, 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.

Activate firewalls and anti-virus software: Firewalls block malicious traffic and anti-virus software scans files for malware.

To learn more about keeping your device safe, see:

- How updates secure your devices (ITSAP.10.096)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Instant messaging (ITSAP.00.266)
- Firewall security considerations (ITSAP.80.039)

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.

Fact check: Scammers also use misinformation to further promote phishing scams. They hope to provoke an emotional response in the reader, such as shock or outrage. However, the information may not be true. Before clicking on links or responding to messages, fact check the information and domain name.

To learn more about social engineering and how to recognize it, see:

- Social engineering (ITSAP.00.166).
- Spotting malicious emails (ITSAP.00.100)
- Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101)
- What is voice phishing (vishing) (ITSAP.00.102)
- How to identify misinformation, disinformation, and malinformation (ITSAP.00.300)

Wi-Fi security and virtual private networks

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. To learn more see, Virtual private networks (ITSAP.80.101)

Wifi hardware

Consider the hardware that your Wi-Fi is connected to, especially when you're working remotely. Routers not supported by your organization, like those in your home, are your responsibility to secure and maintain. Just like every other piece of hardware, routers will eventually reach end -of-life (EOL). Devices that have reached EOL pose a security risk to your organization. EOL means that the vendor stops marketing, selling, and providing support and updates to the device. When you use devices that are not updated to the latest firmware, you can open yourself up to cyber attacks. Firmware is the software that is installed and updated by the manufacturer and contains important security measures. You can check whether your router is EOL by looking at the vendors end-of-life product list or accessing the routers records in its system logs. If it hasn't been updated in several months, it might be time to consider a new router. If unsure, contact your organization's IT department for guidance. To learn more, see Router cyber security best practices (ITSAP.80.019), and Obsolete products (ITSAP.00.095)

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada