TELEWORK SECURITY ISSUES

March 2019 **ITSAP.10.016**

Telework is a flexible and convenient work arrangement that allows you to work outside of the traditional office environment. By remotely connecting to your organization's network, you can continue to use applications and access information as though you were in the office.

SECURITY ISSUES OF TELEWORKING

When you use business equipment outside of your organization's IT security perimeters, it can create a weak link in your organization's overall IT infrastructure. If it is not properly protected, these remote connections can be exploited by threat actors. It is important to protect your mobile devices, as well as any sensitive information and data—whether at rest or in transit. Threats can potentially jeopardize the confidentiality, the integrity and the availability of the information.

TELEWORKING RISKS

Be aware that teleworking increases the possibility of:

- Physical access to your device by unauthorized users which could lead to tampering, breakage, or theft.
- Malicious code being inserted into your device. This can lead to:
  - Traffic manipulation (an attacker inserts their own traffic to influence data and obtain access to the mobile device or the organization's network).
- Social engineering whereby threat actors trick you into sharing information or granting access to your device.
- Compromised login credentials, forgetting your password, weak security settings, etc.
- Compromised communications links through:
  - Eavesdropping—an attacker listens to Wi-Fi or network traffic or records on-line activity. This can include capturing your username and passwords.
  - Theft of service—where an attacker tries to use a teleworker's internet service or processing power for their own purposes (e.g. sending out spam), but has no interest in the transmitted traffic.

In general, there are **two things** that need protection when working offsite: the device and the communications link. Different safeguards should be considered when using personal and corporate devices for teleworking.

SAFEGUARDS FOR PERSONAL DEVICES:

- Restrict computer use to you only (i.e. do not allow family members or others to use your account created for Telework use)
- Comply with business data storage policies, always store business data in approved cloud or local storage
- Implement full disk encryption, in case your computer is stolen or lost
- Use trusted anti-malware software that provides real-time protection as well as (minimum) full disk weekly scans
- Use password-enabled screensavers that activate with user inactivity
- Ensure that your operating system and applications are receiving regular patch updates
- Secure your home wireless router with strong passphrases, WPA-2 encryption (not the insecure WEP encryption) and MAC addressing if possible
- While at a hotel, secure your device by locking it up in the room safe or front desk safe; never leave it unattended in a hotel room
- Use a lock to physically secure portable computers from theft, whenever unattended
- Never use unapproved, unencrypted USB drives or portable hard drives to store business information.
- Use strong identification and authentication such as public key infrastructure (PKI) or two-factor authentication, not just the traditional user-name and password
- Dispose of printouts with sensitive information using an approved shredder or deposit in a secure shredding bin at your workplace
- Do not leave sensitive data which can be accessed or copied on an unsupervised computer
- Turn off Wi-Fi and Bluetooth networking services when not in need and while travelling on public transportation
- Report suspicious, suspected and actual security events to your IT security team immediately

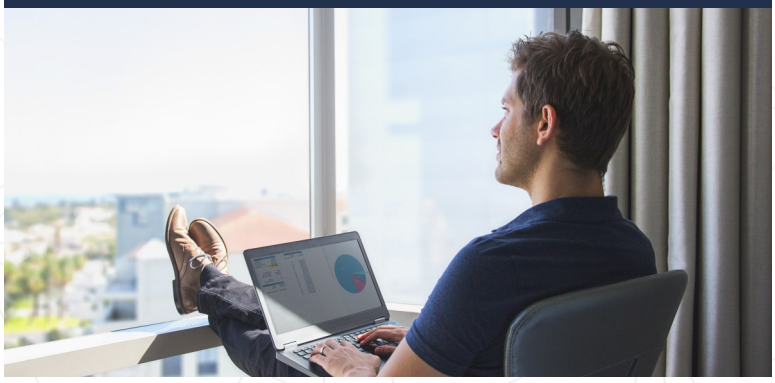
SAFEGUARDS FOR CORPORATE DEVICES:

Your organization's IT department may perform security actions on your device and connection (If your organization does not, ensure you follow the Safeguards for Personal devices). These actions may include:

- Regular monitoring and maintenance of your device
- Configuring and updating operating software, primary applications and security software
- Using network security systems to monitor traffic
- Using firewalls to block unauthorized traffic

Additionally, please remember:

- Use your device for work related matters only and not for personal use
- Do not install or configure software or hardware on your device
- Learn how to safely use the device issued to you
- Always follow your organization's security policy and understand your security obligations
- Never connect an unencrypted USB key or other peripheral to your device
- Back up information on your device to prevent work loss
- Ensure that the information on your device is encrypted when at rest
- Access unclassified or non-sensitive information only
- Follow your employers data storage policies
- Always connect to your organization's network using the provided equipment to establish a secure encrypted channel through a virtual private network (VPN)



Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (CCCS) at **cyber.gc.ca**