USING YOUR MOBILE DEVICE SECURELY

DECEMBER 2020 ITSAP.00.001

Your mobile device provides a convenient and flexible way to work from anywhere or at anytime. While mobile devices play a significant role in the day-to-day operations of organizations and agencies, their use can also pose a threat to information and networks.

Mobile devices are attractive targets that provide unique opportunities for threat actors intent on gathering information because they contain vast amounts of sensitive and personal information. A compromised device has the potential to allow unauthorized access to your organization's network, placing not only your own information at risk, but also that of the organization.

It is important for all employees to remember that Canada is an attractive target for threat actors due to its wealth, resources, and diplomatic relationships.

WHAT IS THE MOBILE THREAT ENVIRONMENT?

The world faces a vastly different cyber-threat environment than that of just 5 years ago. The threats are constantly changing, and firewall, anti-malware, and anti-virus products tend to be a step behind. To defend ourselves, we must keep the following in mind:

- Threat actors evolve quickly—so must our defences.
- Hacking technology is free, easy to use, and widely available.
- Mobile devices are increasingly targeted by sophisticated threat actors.
- Mobile devices are valuable assets to hackers due to the potentially sensitive information stored on them.

WHO IS BEING TARGETED?

Employees at any level can be potential targets, but those frequently targeted include the following individuals:

- Senior executives and their assistants
- Help desk staff and system administrators
- Users who have access to sensitive information
- Users with remote access
- Users whose job involves interacting with members of the public

HOW ARE PEOPLE, PROJECTS, AND SYSTEMS BEING TARGETED?

Threat actors who are looking to gather information on employees, projects, and systems use many different methods:

- Remotely accessing and controlling your device
- Physically tampering with your device
- Using the location tracking function in your mobile device to determine your location
- Sending text messages with malicious links

Did you know?

Technology exists that allows hackers to turn on and control your device — without your knowledge.

AWARENESS SERIES

WHAT CAN I DO?

There are a few simple actions you can take to drastically reduce the risk of exposing sensitive or personal information:

- Use a PIN or passphrase to protect your device.
- Disable features not in use, such as GPS, Bluetooth, or Wi-Fi.
- Avoid joining unknown, unsecured, or public Wi-Fi networks.
- Delete all information stored on a device prior to discarding it.
- Avoid opening files, clicking links, or calling numbers contained in unsolicited text messages or emails.
- Maintain up-to-date software, including operating systems and applications.
- Check privacy policies and user reviews on applications before downloading to ensure they are reliably sourced.
- Do not use "Remember Me" features on websites and mobile applications – always type in your username and passphrase or password to log in.
- Encrypt personal or sensitive data and messages.
- Understand the risks, keep track of your devices (including of cables, chargers and peripherals), and maintain situational awareness.

AM I A TARGET?

There are many different ways to gain access to the information being stored on or transmitted by a mobile device. You need to remain aware of your surroundings when using your device and be on guard while using the Internet and downloading applications. And you need to remember that yes, you are a target.

TRAVELLING WITH A DEVICE?

You should carefully consider the potential risks of using mobile devices while travelling outside of Canada. If travelling with organization-owned devices, be aware of the policies on travelling with mobile devices, and consider the following tips:

- There are steps to take **before**, **during,** and **after** you travel to increase the security of the information stored on your mobile devices.
- In some countries, hotel business centre and phone networks are monitored, and rooms may even be searched.
- Senior executives and those working with valuable information are at a higher risk of being targeted through their mobile devices.
- Mobile devices are a prime target for theft. If stolen, the information contained within may be accessed and used for malicious purposes.

If you will be travelling abroad, consult ***ITSAP.00.087 Mobile Devices and Business Travelers*** for valuable information on protecting your mobile device before, during, and after travel.

WHERE CAN I LEARN MORE?

The Cyber Centre has created additional publications that provide guidance on how to use your mobile device. Some publications include:

- *ITSM.80.001 Securing the Enterprise for Mobility*
- *ITSAP.30.032 Best Practices for Passphrases and Passwords*
- *ITSAP.30.030 Secure Your Accounts and Devices With Multi-Factor Authentication*
- *ITSAP.00.015 Have You Been Hacked?*
- *ITSAP.10.116 Cyber Security Tips for Remote Work*
- *ITSAP.70.015 Security Tips for Peripheral Devices*
- *Cyber Security and Wireless Technologies (online quiz)*

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 (Cyber Centre) at **cyber.gc.ca**