CANADIAN CENTRE FOR CYBER SECURITY

Using your mobile device securely

October 2024

ITSAP.00.001

Your mobile device provides an easy way to work from anywhere, at any time. While they play an important role at work, they can pose a threat to your organization's information and networks, if compromised.

The mobile threat environment

The cyber threat environment is changing very quickly. Threats are constantly evolving, and threat actors can:

- leverage new and evolving tactics and techniques
- access easy to use and widely available hacking tools

Mobile devices are prime targets for threat actors who want to gather information about you or your organization. A compromised device could allow threat actors to access your organization's network and obtain its information.

Did you know?

Hackers can use existing technology to turn on and control your device without your knowledge.

Targets

Canadian organizations and individuals are prime targets for threat actors due to Canada's wealth, resources, and strong relationships with other countries. Employees at any level can be potential targets, but threat actors frequently target:

- senior executives and their assistants
- help desk staff and system administrators
- users who have access to sensitive information
- users with remote access
- users who deal with members of the public

Targeting methods

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

- remotely accessing and controlling your device
- physically tampering with your device
- using your mobile device's tracking function to determine your location
- sending messages by SMS, email, or social media with malicious links
- sending e-mails containing links to malicious websites

AWARENESS SERIES

Cat. No. D97-1/00-001-2024E-PDF
ISBN 978-0-660-72985-5

Taking action to protect your mobile devices

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

- Connect through a VPN wherever possible
- Use a PIN or password to protect your device
- Deactivate features when 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 e-mails
- Update software, including operating systems and applications
- Check privacy policies and user reviews on applications before downloading to ensure they are reliable
- Use unique and complex passphrases or passwords and activate multi-factor authentication (MFA), if available
- Avoid using free password managers that are not part of your operating system or browser
- Limit the use of "remember me" features on websites and mobile applications – if MFA is not available, type in your username and passphrase or password to log in for important accounts
- Use encryption features to secure personal or sensitive data and messages
- Keep track of your devices, including cables, chargers, and peripherals

Remember, you are a target!

There are many ways to gain access to the information stored on or transmitted by a mobile device. You need to remain aware of your surroundings when using your device and be vigilant while using the Internet and downloading applications. Remember, anyone can be a target – including you.

Considerations when travelling with your device

You should carefully consider the risks of using mobile devices while travelling outside of Canada. Know your organization's policies on travelling with corporately owned mobile devices and take note of the following:

- Increase the security of the information stored on your device by following your organization's mobile device travel policies before, during and after you travel.
- In some countries, hotel business centres and phone networks are monitored and rooms may even be searched.
- Senior executives and those working with valuable information are at higher risk of being targeted through their mobile devices
- Mobile devices are a prime target for theft and, if stolen, the information they contain may be accessed and used for malicious purposes.

Consult Mobile devices and business travellers (ITSAP.00.087) for more information on travelling with your device.

Learn more

- Cyber security at home and in the office: Secure your devices, computers, and networks (ITSAP.00.007)
- Securing the enterprise for mobility (ITSM.80.001)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
- Cyber security tips for remote work (ITSAP.10.116)
- Security tips for peripheral devices (ITSAP.70.015)
- How updates secure your device (ITSAP.10.096)