Using Your Mobile Device Securely

JUNE 2016 | AWARENESS SERIES | ITSAP.00.001

As an employee of the Government of Canada (GC) your mobile device provides a convenient and flexible way to work anywhere or at anytime. While mobile devices play a vital role in the day-to-day operations of GC departments and agencies, their use also poses a threat to GC information and networks.

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

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

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 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 being increasingly targeted by sophisticated threat actors.
- Mobile devices are valuable assets to a hacker due to the potentially sensitive information stored on them.

Did you know?

Technology exists that a hacker can use to turn on and control your device – without your knowledge.

Who is Being Targeted?

As an employee of the GC, you are privy to important and sensitive information. While every employee at any level can be a potential target, high-value and frequently targeted employees tend to include:

- 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 role involves interacting with members of the public.

HOW?

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

- 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.
- Sending e-mails containing links to malicious websites or phishing attempts.

Canada

Using Your Mobile Device Securely

JUNE 2016 | AWARENESS SERIES | ITSAP.00.001

What can I do?

There are a few simple actions that employees can take to drastically reduce the risk of exposing sensitive GC or personal information, including:

- Use a PIN or password to access the device.
- Disable features not in use such as GPS, Bluetooth, or Wi-Fi.
- Avoid joining unknown or unsecured 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.
- Maintain up-to-date software, including operating systems and applications.
- Do not use "Remember Me" features on websites and mobile applications – always type in your password.
- Encrypt personal or sensitive GC data and messages.
- Understand the risks, keep track of your devices, and maintain situational awareness.

Travelling with your Device

You should carefully consider the potential risks of using mobile devices during travel outside of Canada. Be aware of your department's policies regarding travelling with GC mobile devices, and consider the following:

- 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 centers and phone networks are monitored and rooms may even be searched.
- Senior officials 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. If stolen, the information contained within may be accessed and used for malicious purposes.

If you will be travelling abroad, please take a minute to download CSE's *Mobile Technologies in International Travel* for valuable information on protecting your mobile device before, during, and after travel.

If you would like to learn more, sign-up for CSE's Wireless Security course (#350).

WE ARE CYBER SECURITY

REMEMBER, YOU ARE 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 constantly be on guard while using the internet and downloading applications.

CONTACT US

www.cse-cst.gc.ca/its

itsclientservices@cse-cst.gc.ca

Canada