CYBERHYGIENE

MOBILE SECURITY

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

It is important to remember that Canada is an attractive target for cyber-threat actors.

- Use a PIN or password to access the device and change these passwords regularly
- Disable features not in use such as GPS, Bluetooth, or Wi-Fi
- 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 ID and password
- Encrypt personal or sensitive data and messages
- Understand the risks, keep track of your devices, and maintain situational awareness
- Review and understand the privacy and access requirements of all apps before installing them on mobile devices
- Delete all information stored on a device prior to discarding it
- Do important tasks, like online banking on a private or known, trusted secure network

PASSWORDS

- Try using a memorable phrase to create a stronger password using a mix of characters. For example:

  "*My jersey number when I played sports was 27!*"
  PASSWORD: **Mj#wIpsw27!**
- Be wary of your surroundings and always shield your keyboard or keypad when entering your password
- Use different passwords for work and home accounts
- Do not write your passwords under a keyboard, on sticky notes next to a computer or save them on the device itself as these are common places to look for passwords
- If at any time you suspect that your password may have been compromised, act quickly and change it
- Change passwords after returning from travel

E-MAIL SPEAR PHISHING

Spear phishing is a tactic that uses social engineering to tailor e-mails to individuals or groups based on their line of work, interest, or personal characteristics. Spear phishing e-mails will be about a subject that is relevant to the recipient and will appear to be sent by a credible source.

HOW TO DETECT A SPEAR PHISHING E-MAIL

Before opening attachments or clicking on links, ensure that:

- You really know who is sending the e-mail and that the tone is consistent for the sender
- The content is really relevant to your work and not just related to your area of interest
- The web address or attachment is relevant to the content of the e-mail
- You use extra caution if the e-mail is from a personal address (**@YAHOO.CA**, **@GMAIL.COM**) or a suspicious domain

SOCIAL MEDIA TIPS

- Use a unique password for every account
- Ensure all available security and privacy options have been applied on your account
- Review your account's website security and privacy policies regularly for changes
- Be careful when accessing unknown website links or attachments
- Report any suspected security incidents to your IT support team
- Use judgement when posting personal information on social media platforms for both privacy and cyber security reasons

QUICK REFERENCE GUIDE (IN CANADA)

Understand the security measures that exist on your devices.

- **VOICE COMMUNICATION:**
  Acceptable for non-sensitive information only
- **TEXTS AND MESSAGING APPS:**
  NOT acceptable for any sensitive communications
- **E-MAIL:**
  Consult your IT support team before using your email for sensitive communications

TRAVELLING WITH YOUR DEVICE

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 centres 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
- Use a separate device specifically for travel purposes only — don't use your regular business or personally owned device
- Don't use storage devices (ex: USB key) given to you, or purchased from unknown sources
- Avoid using your own USB key in a foreign computer
- Only use the charging equipment you brought

GENERAL PREVENTION

- **PATCH AND UPDATE DEVICES REGULARLY:**
  Having the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats. To defend against known risks, turn on automatic updates if that's an available option.
- **PROTECT INTERNET CONNECTED DEVICES:**
  Use 2-step verification and basic security products, like anti-virus programs on web-enabled devices, to protect from viruses, malware, and unauthorized access.
- **WI-FI NETWORKS:**
  Avoid joining public, unknown, or unsecured Wi-Fi networks.
- **BACK UP IMPORTANT DATA:**
  Always back up important data on a separate local storage device.
- **ACT QUICKLY:**
  If you are notified, become aware, or even just suspect your computer is infected, notify your IT support team.

WE ARE
CYBER SECURITY

CONTACT US
cse-cst.gc.ca/its
itsclientservices@cse-cst.gc.ca

Canada