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.

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

Centre de la sécurité des télécommunications | Communications Security Establishment

NON CLASSIFIÉ

PRATIQUES EXEMPLAIRES EN CYBERSÉCURITÉ

SÉCURITÉ DES DISPOSITIFS MOBILES

Les dispositifs mobiles sont des cibles attrayantes qui offrent des occasions uniques aux auteurs de menaces qui cherchent à recueillir de l'information. Un dispositif compromis peut fournir un accès non autorisé au réseau de votre ministère, ce qui menace à la fois la sécurité de votre information et celle de votre ministère.

Il est important de se rappeler que le Canada est une cible de choix pour les auteurs de cybermenaces.

- Utilisez un numéro d'identification personnel (NIP) ou un mot de passe pour accéder à vos dispositifs, et changez vos mots de passe régulièrement
- Désactivez les fonctions que vous n'utilisez pas, comme le GPS, le Bluetooth ou le Wi-Fi
- Évitez d'ouvrir des fichiers, de cliquer sur des liens ou d'appeler des numéros contenus dans des textos ou des courriels non sollicités
- Gardez vos logiciels à jour, y compris les systèmes d'exploitation et les applications
- N'utilisez pas la fonction « se souvenir de moi » des sites Web et des applications mobiles — tapez toujours votre nom d'utilisateur et votre mot de passe
- Chiffrez les données et les messages personnels ou sensibles
- Comprenez les risques, surveillez vos dispositifs et demeurez conscient de la situation
- Passez en revue les exigences en matière d'accès et de protection de la vie privée de toutes les applications avant de les installer sur des dispositifs mobiles, et assurez-vous de bien les comprendre
- Supprimez toute l'information stockée dans votre dispositif avant de vous en débarrasser
- Réalisez les tâches importantes, comme les transactions bancaires en ligne, sur un réseau privé ou fiable

MOTS DE PASSE

- Essayez d'utiliser une phrase facile à retenir pour créer un mot de passe robuste qui comporte divers caractères. Par exemple :

  « Je n'aime pas les saucisses! »
  MOT DE PASSE : **jnMp@lés06!**
- Soyez conscient de votre environnement et cachez toujours votre clavier lorsque vous y entrez votre mot de passe
- Utilisez des mots de passe différents au travail et à la maison
- N'écrivez pas vos mots de passe sous un clavier, sur une note autocollante près de votre ordinateur ou dans un fichier enregistré sur votre dispositif, car ces endroits sont bien connus de ceux qui cherchent des mots de passe
- Si vous soupçonnez que votre mot de passe a été compromis, n'attendez pas : changez-le immédiatement
- De retour de voyage, changez vos mots de passe

COURRIELS DE HARPONNAGE

Le harponnage est une tactique qui emploie les techniques de piratage psychologique pour façonner les courriels malveillants en fonction de la profession ou des intérêts des destinataires, ou de caractéristiques propres à ces derniers. Ainsi, de tels courriels portent sur des sujets d'intérêt pour leurs destinataires et semblent provenir d'une source crédible.

COMMENT PEUT-ON REPÉRER UN COURRIEL DE HARPONNAGE?

Avant d'ouvrir une pièce jointe ou de cliquer sur un lien :

- Sachez précisément qui est l'expéditeur du courriel et assurez-vous que le ton employé correspond à ce que l'on pourrait s'attendre de l'expéditeur en question
- Assurez-vous que le contenu convient vraiment à la nature de son travail et ne fait pas simplement référence à des intérêts personnels
- Vérifiez si l'adresse Web ou le fichier joint correspond au contenu du courriel
- Faites preuve d'une extrême prudence si le courriel provient d'un compte courriel personnel (**@YAHOO.CA**, **@GMAIL.COM**) ou d'un domaine suspect

CONSEILS CONCERNANT LES MÉDIAS SOCIAUX

- Utilisez un mot de passe unique pour chacun de vos comptes
- Appliquez à votre compte toutes les options de sécurité et de confidentialité
- Consultez régulièrement les politiques de sécurité et de confidentialité du site Web de votre compte pour prendre connaissance de tout changement apporté
- Soyez vigilant lorsque vous cliquez sur des liens dans des sites Web inconnus ou lorsque vous ouvrez des pièces jointes à partir de ces sites Web
- Signalez tout incident de sécurité suspect à votre équipe des TI
- Pour des raisons de confidentialité et de cybersécurité, faites preuve de jugement lorsque vous publiez des renseignements personnels sur les médias sociaux

GUIDE DE RÉFÉRENCE RAPIDE (AU CANADA)

Assurez-vous de bien comprendre les mesures de sécurité de vos dispositifs.

- **COMMUNICATION VOCALE :** Acceptable pour l'information non sensible uniquement.
- **TEXTOS ET APPLICATIONS DE MESSAGERIE :** INACCEPTABLE pour toute communication sensible.
- **COURRIELS :** Consultez votre équipe de soutien TI avant d'utiliser votre compte courriel pour les communications sensibles.

VOYAGER AVEC VOTRE DISPOSITIF

Vous devez prendre des mesures **AVANT**, **PENDANT** et **APRÈS** votre voyage afin d'accroître la sécurité de l'information stockée sur vos dispositifs mobiles.

- Dans certains pays, les centres d'affaires et les réseaux téléphoniques des hôtels sont surveillés, et les chambres d'hôtel sont même parfois fouillées
- Les dispositifs mobiles des hauts fonctionnaires ou des personnes qui travaillent avec de l'information importante risquent plus d'être ciblés que les dispositifs d'autres employés
- Les dispositifs mobiles sont des cibles de choix pour les voleurs — si un voleur s'en empare, il pourrait accéder à l'information qu'ils contiennent, puis l'utiliser à des fins malveillantes
- Utilisez un dispositif distinct réservé aux voyages; n'utilisez pas votre dispositif personnel ni celui que vous utilisez régulièrement au travail
- N'utilisez pas les dispositifs de stockage (p. ex. clés USB) qui vous sont donnés par des sources inconnues ou que vous achetez de sources inconnues
- Évitez d'utiliser votre propre clé USB dans un ordinateur étranger
- Utilisez uniquement les chargeurs que vous avez apportés
- De retour de voyage, changez vos mots de passe

PRÉVENTION GÉNÉRALE

- **INSTALLEZ RÉGULIÈREMENT LES CORRECTIFS ET LES MISES À JOUR NÉCESSAIRES SUR VOS DISPOSITIFS**
  En téléchargeant les dernières versions des logiciels de sécurité, des navigateurs Web et des systèmes d'exploitation, vous prenez les meilleures mesures de protection contre les virus, les maliciels et les autres menaces en ligne.

  Pour vous protéger contre les risques connus, activez les mises à jour automatiques si vous avez cette option.
- **PROTÉGEZ LES DISPOSITIFS CONNECTÉS À INTERNET**
  Utilisez la vérification à deux étapes et des produits de sécurité de base, comme des programmes antivirus, sur les dispositifs Web pour les protéger contre les virus, les maliciels et les accès non autorisés.
- **RÉSEAUX WI-FI**
  Évitez de vous connecter à des réseaux Wi-Fi publics inconnus ou non sécurisés.
- **SAUVEGARDEZ LES DONNÉES IMPORTANTES**
  Sauvegardez toujours les données importantes sur un dispositif de stockage local distinct.
- **AGISSEZ RAPIDEMENT**
  Si l'on vous avise que votre ordinateur a été compromis ou si vous vous rendez compte ou soupçonnez qu'il a été compromis, veuillez en aviser l'équipe des TI.

NOUS SOMMES LA **CYBERSÉCURITÉ**

COMMUNIQUEZ AVEC NOUS À
cse-cst.gc.ca/fr/its
itsclientservices@cse-cst.gc.ca

Canada