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 du 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.