UNITÉ PRÉVENTION
SERVICE DE POLICE DE LA VILLE DE QUÉBEC

En sécurité sur Internet

Information à l'intention des citoyens

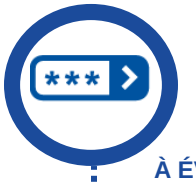
{ fiche info }

INTRODUCTION

Nous en sommes tous conscients, le « cybermonde » fait désormais partie de notre quotidien. Il a investi nos vies, notre maison, notre bureau et s'immisce jusque dans les moindres recoins de nos déplacements et agissements. S'il s'est d'abord présenté comme un outil de communication révolutionnaire, Internet est désormais reconnu comme un monde à part entière. Il possède ses propres acteurs, son propre langage, ses propres valeurs. Et bien qu'il offre un éventail impressionnant d'opportunités pour le développement économique et l'enrichissement des connaissances, il peut aussi être un partenaire de crime redoutablement efficace : toujours disponible, toujours à l'affut, toujours prêt à agir et souvent anonyme.

Que faire

POUR VOUS PROTÉGER?



UTILISEZ DES MOTS DE PASSE DE QUALITÉ

La force d'un mot de passe dépend de **sa longueur** et du nombre de **possibilités existantes** pour chacun des caractères.

Mot de passe composé de lettres minuscules et majuscules, de chiffres et de caractères spéciaux.
Exemple : **3Maisons&7Chevaux**

Mot de passe mnémotechnique.
Exemple : **un tien vaut mieux que deux tu l'auras : 1tvmq2tl'A**

À ÉVITER

- Utiliser un mot de passe ayant un lien avec votre **vie personnelle** (nom, date de naissance, etc.).
- Utiliser le **même mot de passe** pour des accès différents.
- **Noter vos mots de passe** dans votre ordinateur.
- Configurer votre système pour qu'il enregistre **automatiquement** les mots de passe.

Saviez-vous que?

Les mots de passe les plus souvent utilisés sont :

1. password
2. 123456
3. 1234567
4. 1234
5. qwerty
6. 12345

INSTALLEZ DES LOGICIELS DE PROTECTION À JOUR

La plupart des attaques tentent d'utiliser les failles d'un ordinateur, ce qui est le cas notamment lorsque les logiciels de protection ne sont pas à jour (navigateur, antivirus, pare-feu personnel et filtre de courriel).

CONTRÔLEZ LA DIFFUSION DE VOS INFORMATIONS PERSONNELLES

Avant de saisir vos informations personnelles (comme des coordonnées bancaires), assurez-vous que le site Internet est sécurisé. Un cadenas apparaît dans le navigateur et l'adresse du site commence par HTTPS au lieu de HTTP.

SOYEZ VIGILANT AVANT D'OUVRIR LES PIÈCES JOINTES

Ne cliquez pas directement sur le lien : saisissez vous-même l'adresse du site dans la barre d'adresse du navigateur.

Par ailleurs, n'ouvrez jamais les pièces jointes dont les extensions sont les suivantes :
.pif .bat .exe .vbs .lnk.

EFFECTUEZ DES SAUVEGARDES RÉGULIÈRES

En conservant une copie de vos données, vous pourrez réagir à une attaque ou un dysfonctionnement de votre ordinateur. La sauvegarde de vos données est une condition de la continuité sécuritaire de votre activité.

Saviez-vous que?

Le Service de police de la ville de Québec dispose d'une **équipe formée pour saisir les preuves stockées** sur les ordinateurs des victimes de fraude par Internet.

63 % des utilisateurs canadiens ont déclaré avoir déjà eu un **virus** informatique. Parmi ces personnes, 49 % ont précisé que le virus avait entrainé une **perte de données.**

37 % des utilisateurs canadiens ont déclaré avoir déjà reçu un **courriel malveillant** les invitant à divulguer des informations personnelles ou des données bancaires.

Le **paiement par carte bancaire est aussi sécuritaire sur Internet** que dans la vie courante, à condition de respecter quelques principes de base.

Source :

Gouvernement du Canada, *Pensez cybersécurité* [en ligne]