alpha numérique

FICHE RÉSUMÉ

Sécurité en ligne : Trucs et Astuces

Introduction

La sécurité en ligne est omniprésente dans l'expérience numérique. Découvrez des trucs et astuces clés en main pour mieux vous protéger et développer de bons réflexes en tant qu'usager. Dans cette fiche, nous verrons quelles sont les données à protéger et découvrirons les outils de base pour garantir notre sécurité en ligne.

Dans ce document, le symbole du cadenas est utilisé pour mesurer approximativement le niveau de protection associé à chaque solution proposée. Moins il y a de cadenas, plus il sera facile de pirater la donnée à protéger si on s'abstient d'utiliser cette solution de protection.

Quelles sont les données personnelles que j'ai à protéger ?

DES DONNÉES À PROTÉGER PEUVENT ÊTRE ENREGISTRÉES DANS MON APPAREIL.

- Numérisation de documents administratifs.
- Données ou photos privées.
- Données professionnelles délicates.

J'AI LE DROIT DE LAISSER UN MINIMUM DE TRACES LORS DE « MES BALADES » EN LIGNE.

- Mon identité.
- Les achats que j'effectue.
- Les sites internet que je visite.

J'UTILISE INTERNET POUR COMMUNIQUER CONSCIEMMENT DES DONNÉES PERSONNELLES.

- Courriels
- Suivi de mes comptes en banque et en agences gouvernementales
- Communications sur les réseaux sociaux

Comment protéger mon appareil ?

Je dois m'assurer que mon appareil reste en ma possession et que personne de mal intentionné ne puisse y avoir accès.

- Attention aux appareils laissés sans surveillance.
- Attention aux appareils que l'on transporte partout.
- Penser aux solutions de localisation et verrouillage à distance.

Je dois utiliser des mots ou PHRASES de passe pour verrouiller mon appareil et mes logiciels.

- Pour votre appareil, pensez aux paramètres associés au mot de passe comme le temps avant verrouillage.
- Pour les logiciels, pensez aux gestionnaires de mot de passe comme *Keepass* (gratuit), *LastPass* (gratuit)…
- Bien que plus contraignante, la double authentification renforce la sécurité.

Je peux utiliser un antivirus (ex. : *Avira, BitDefender, Avast*).

- Protection des logiciels malveillants *(malware).*
- Protection des virus espions *(spyware).*
- Protection des entrées et sorties dans mon ordinateur : Pares-feux.

Je peux crypter les fichiers trop sensibles que je garde sur mon appareil.

- Le cryptage s'apparente à un coffre-fort numérique.
- Il existe des logiciels de cryptage gratuits (ex. : *AxCrypt, VeraCrypt*)

Comment protéger ma navigation web ?

Je dois naviguer sur internet avec des connexions sécurisées : HTTPS !

- HTTP est un protocole de transfert de données.
- HTTP**S** est la version sécurisée du HTTP.

Je peux refuser l'utilisation des témoins de navigation ou *cookies*.

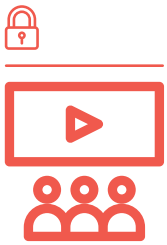
- Les cookies permettent de personnaliser notre expérience d'internet et offre un grand confort de navigation.
- Les cookies dévoilent nos données personnelles et nos habitudes à des compagnies privées.
- L'analyse de ces données comportementales sont vendues et achetées par des compagnies privées.

Si je veux rester anonyme, je peux éviter de me connecter fréquemment avec des identifiants de connexion.

Je peux utiliser des serveurs distants ou *proxys* pour simuler le fait que je me connecte d'ailleurs et ainsi rendre difficile mon traçage par adresse IP.

- Le réseau privé virtuel ou VPN (Virtual Private Network) permet de simuler une connexion d'ailleurs.
- Des navigateurs anonymisant comme Tor utilisent automatiquement plusieurs proxys avant de vous connecter au site Web que vous souhaitez rejoindre.

Comment protéger les données que je souhaite communiquer sur le web ?



Je m'assure de contrôler ou d'être conscient de mon auditoire.

- Qui peut voir l'information que je mets en ligne ?
- A quel point puis-je faire confiance à cette audience ?

Par exemple sur Facebook :

- https://www.facebook.com/settings?tab=privacy
- https://www.facebook.com/settings?tab=timeline
- https://www.facebook.com/settings?tab=followers

J'essaye de m'assurer que le contenu que je communique ne me nuira pas ni ne pourra nuire à autrui.

- Est-il vraiment nécessaire de publier ma date de naissance, mon numéro de téléphone, mon adresse, mon emploi, etc., en ligne ?
- Qui est propriétaire de l'information que je publie sur le site de réseautage social ?
- Quels renseignements à mon sujet mes contacts peuvent-ils transférer à d'autres parties ?

Sur les réseaux sociaux, je peux utiliser différents comptes/pseudonymes en fonction de l'audience à qui je m'adresse (famille, travail, loisirs).

Site antifraude au Canada : https://www.antifraudcentre-centreantifraude.ca/index-fra.htm

Continuez à apprendre sur alphanumerique.ca !