Protéger son empreinte numérique

Qu'est-ce que votre empreinte numérique?

*1 - **L'empreinte de votre doigt utilisée pour déverrouiller vos appareils électroniques?***

*2 - **« Votre « empreinte numérique » comprend l'ensemble des traces de votre activité en ligne, des commentaires postés sur des articles de presse ou sur les réseaux sociaux aux achats en ligne que vous effectuez. »***

Source: https://fr.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html

LA BASE

Trouvez l'intrus

Avoir un mot de passe robuste

Utiliser un Mac plutôt qu'un PC

Utiliser un antivirus

Faire la mise à jour régulière des logiciels fondamentaux

Faire une sauvegarde régulière sur un support externe

Avoir un mot de passe robuste

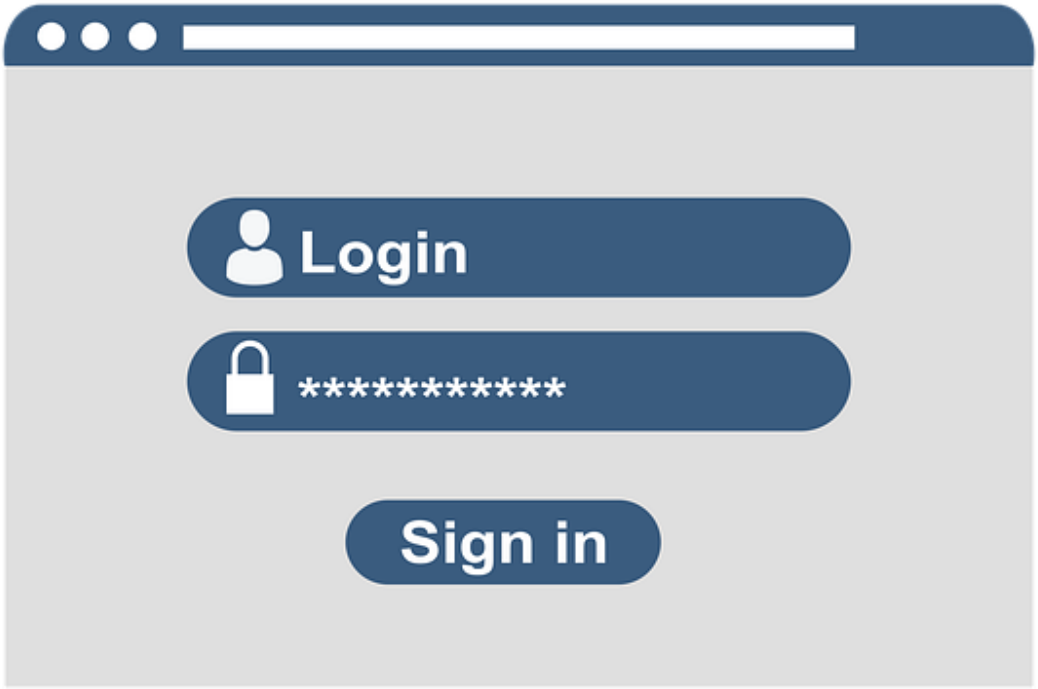
Utiliser un Mac plutôt qu'un PC

Utiliser un antivirus

Faire la mise à jour régulière des logiciels fondamentaux

Faire une sauvegarde régulière sur un support externe

Mot de passe



Quel est le mot de passe le plus sécuritaire?

password

12345678

abc123

Alp,lbt#FB

passw0rd

trustno1

qwerty123

baseball

123mdp

Alp,lbt#FB

Tous les autres sont tirés des listes de mots de passe les plus courants et, par conséquent, les plus faciles à pirater.

Source: https://fr.wikipedia.org/wiki/Liste_des_mots_de_passe_les_plus_courants

Conseils pour un mot de passe robuste :

- long
- incluant des chiffres, des lettres et des caractères spéciaux
- difficile à deviner par quelqu'un d'autre
- différent d'un service à l'autre

3 techniques :

Technique d'association :

ArmoireLampeChaiseTapis

Technique de la première lettre :

Un tiens vaut mieux que deux tu l'auras

1TvmQ2tl'@

Technique de l'approche phonétique :

j'ai acheté huit cd pour cent dollars cet avant-midi

ght8CD%$7am

Sources :

- Capsule "Les mots de passe", Mois de la cybersécurité, Gouvernement du Québec
- Avenues.ca : Bien gérer vos mots de passe[1]
- Mozilla : Créer des mots de passe sûrs pour protéger votre identité[2]

Au besoin, utilisez un gestionnaire de mots de passe,

comme NordPass[3], 1Password[4], Dashlane[5] ou Keeper[6]

[1] https://avenues.ca/decouvrir/techno/bien-gerer-vos-mots-de-passe/
[2] http://mzl.la/19rnfaI
[3] https://nordpass.com/fr/
[4] https://1password.com/fr/

Antivirus

Un antivirus est essentiel!

Si vous ne pouvez en faire l'achat, il existe des antivirus gratuits:

- Avast

---

[5] https://www.dashlane.com/fr/
[6] https://www.keepersecurity.com/fr_FR/

- Kaspersky
- AVG
- Bitdefender
- etc.

Source: https://www.pcmag.com/picks/the-best-free-antivirus-protection

Mise à jour des logiciels fondamentaux

Configurez la mise à jour automatique des logiciels fondamentaux:

- Système d'exploitation (Windows, MacOS, etc.)
- Navigateur (Chrome, Firefox, Edge, Safari, Opera, etc.)
- Antivirus

Un logiciel désuet est vulnérable aux attaques.

Sauvegarde régulière

Sauvegardez **régulièrement** vos fichiers sur un **support externe**,

pas seulement sur votre ordinateur lui-même.

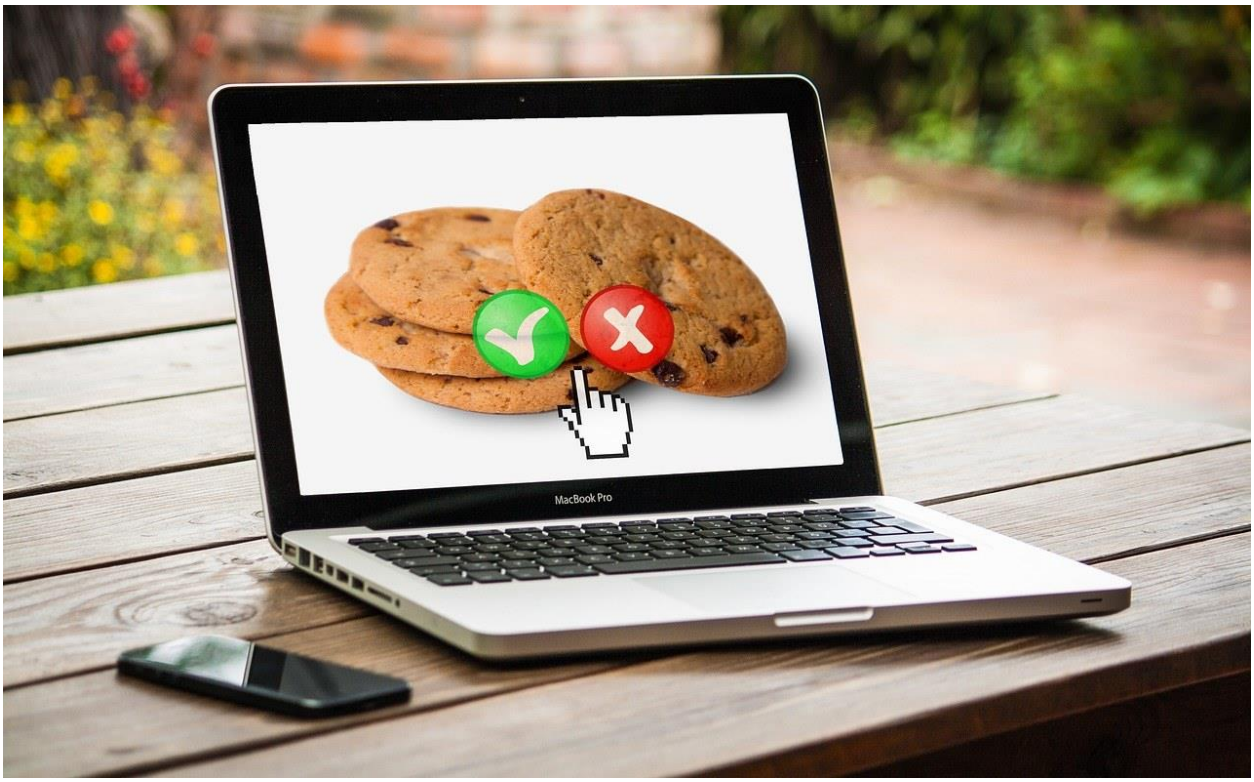
NAVIGATION EN LIGNE

Protocole HTTPS

Un **cadenas** devant l'adresse d'un site web indique que le protocole HTTPS est utilisé. HTTPS est plus sécuritaire que le traditionnel HTTP, car l'information est encryptée.

Attention: C'est plus sécuritaire, mais ce n'est pas infaillible!

Gestion des cookies



Les cookies sont des éléments d'information transmis par le serveur au navigateur lorsque l'internaute visite un site Web, et récupérés par ce serveur lors de visites subséquentes.

Source: Grand dictionnaire terminologique[7]

Ils facilitent la navigation sur ces sites Web,

mais

peuvent enregistrer ce que vous faites pour ensuite montrer des publicités ciblées.

[7] http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=2075216

3 - https://www.lefigaro.fr/

Navigation privée

La navigation privée n'enregistre **pas**:

- les sites Web visités dans l'historique de navigation;
- les cookies;
- les fichiers temporaires;
- les identifiants, mots de passe, etc.

Attention:

- La navigation privée n'offre **aucun anonymat**; l'adresse IP reste visible.
- Les logiciels espions ou malveillants peuvent quand même s'installer sur votre ordinateur.

Choix du moteur de recherche

DuckDuckGo

4 - https://duckduckgo.com/

Startpage

5 - https://www.startpage.com/

Il existe beaucoup de moteurs de recherche alternatifs.

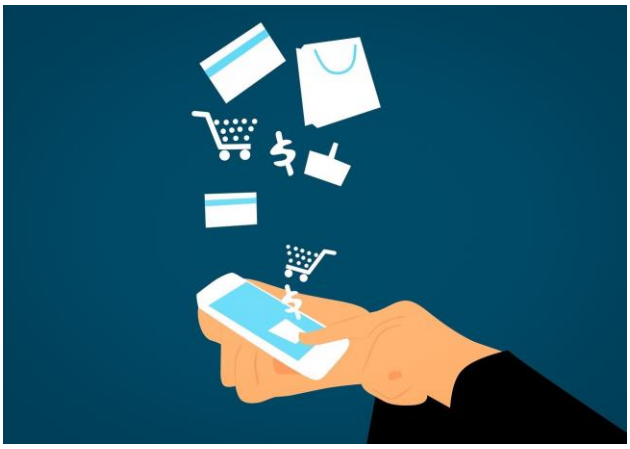
Certains ont une mission sociale (Ecosia[8] pour planter des arbres, Ekoru[9] pour nettoyer les océans, etc.), d'autres se concentrent sur la protection des renseignements personnels.

Pour vous aider à choisir, consultez ces deux[10] listes[11] comparatives des meilleurs moteurs de recherche alternatifs.

[8] https://www.ecosia.org/
[9] https://ekoru.org/
[10] https://kinsta.com/fr/blog/moteurs-recherche-alternatifs/
[11] https://junto.fr/blog/moteurs-recherche-alternatifs/

Réseaux wifi publics

Les réseaux wifi publics sont beaucoup plus risqués que les réseaux privés.



Ne partagez **pas** d'information personnelle sur un réseau wifi public.

Ne faites **jamais** de transactions bancaires en ligne via un réseau wifi public.

Risques liés à l'utilisation d'un wifi public :

Écoute clandestine :

Quand une personne intercepte les communications entre deux parties.

Infection par un programme malveillant :

Infecté par un autre appareil connecté au même réseau, ou encore le point d'accès wi-fi lui-même peut être infecté

Leurre :

Le réseau public auquel on tente d'accéder simule l'apparence d'un réseau légitime, alors qu'il a été créé par un pirate dans le but de voir transiter des informations.

Source :

Capsule "Utiliser un réseau public", Mois de la cybersécurité, Gouvernement du Québec

VPN

VPN = Virtual Private Network

« Réseau de communication privé et sécurisé qui se sert de l'infrastructure d'un réseau public pour transmettre des données protégées, généralement par chiffrement ou encapsulation. »

Source : Termium Plus[12]

Gratuit ou payant?

Gratuit

Attention! Beaucoup de VPN gratuits collectent vos données et ne vous protègent pas vraiment.

- Bons VPN gratuits : ProtonVPN[13], PrivadoVPN[14], Hide.me[15], Windscribe[16], TunnelBear[17]
- Fonctions limitées
- **La meilleure option :** profiter de l'essai gratuit d'un bon VPN payant

Payant

- Nombre de serveurs et leur géolocalisation, protocole de sécurité, bande passante, nombre d'appareils supportés, soutien aux usagers, application mobile, confidentialité des données et juridiction de l'entreprise, accès aux plateformes de diffusion en continu, prix
- Période d'essai gratuit
- Express VPN[18], Nord VPN[19], Cyberghost[20], SurfShark[21], Private Internet Access[22], etc.

---

[12] https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=1&srchtxt=vpn&index=alt&codom2nd_wet=UC#resultrecs
[13] https://protonvpn.com/fr/
[14] https://privadovpn.com/fr/
[15] https://hide.me/fr/
[16] https://fra.windscribe.com/
[17] https://www.tunnelbear.com/
[18] https://www.expressvpn.com/fr
[19] https://nordvpn.com/fr/
[20] https://www.cyberghostvpn.com/fr_FR/
[21] https://surfshark.com/fr/
[22] https://fra.privateinternetaccess.com/

CRÉATION & GESTION DES COMPTES

Remplissez seulement les champs obligatoires d'un formulaire.

Ils sont habituellement marqués d'un astérisque.

Utilisez des adresses courriel différentes pour différents besoins.

Ne connectez pas votre compte Facebook ou Google à un autre service.

Paramétrez la confidentialité de vos comptes Facebook, Google et autres.

N'oubliez pas de vous **déconnecter** de vos comptes en ligne après avoir utilisé un ordinateur public.

HAMEÇONNAGE

« Technique de fraude basée sur l'usurpation d'identité, qui consiste à envoyer massivement un message en se faisant passer pour une institution financière ou une entreprise commerciale de renom afin d'induire les destinataires en erreur et de les inciter à révéler des informations sensibles à leur insu. »

Source: Grand dictionnaire terminologique[23]

Reconnaître l'hameçonnage:

- Validez l'adresse courriel de l'expéditeur
- Survolez l'hyperlien proposé pour voir vers quel site Web ça mène... **sans cliquer dessus!**
- Vérifiez l'orthographe et la grammaire du message
- Méfiez-vous des communications génériques : *Cher client...*
- Validez si la signature correspond à l'adresse courriel

[23] http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8869710

- Vérifiez si on fournit une façon de contacter l'expéditeur, autre que par courriel
- Évaluez le contenu du message: **pourquoi est-ce urgent?**

Quoi faire?

- Ne pas cliquer sur les liens
- Ne pas répondre au courriel ni le transférer
- Contacter la personne ou l'organisme concerné par d'autres moyens
- Dénoncer la fraude auprès des autorités[24]

MERCI!

N'oubliez pas de compléter le formulaire d'appréciation[25], svp (URL dans le clavardage).

Pour recevoir la présentation[26], envoyez-moi votre adresse courriel à activitesnumeriques@banq.qc.ca[27] ou inscrivez-la dans le clavardage.

Toutes les images proviennent de https://pixabay.com/fr/

[24] https://www.antifraudcentre-centreantifraude.ca/index-fra.htm
[25] https://forms.office.com/r/fGMRPcEvt1
[26] https://sway.office.com/fGBeXm4k5EulXx7d?ref=Link
[27] mailto:activitesnumeriques@banq.qc.ca