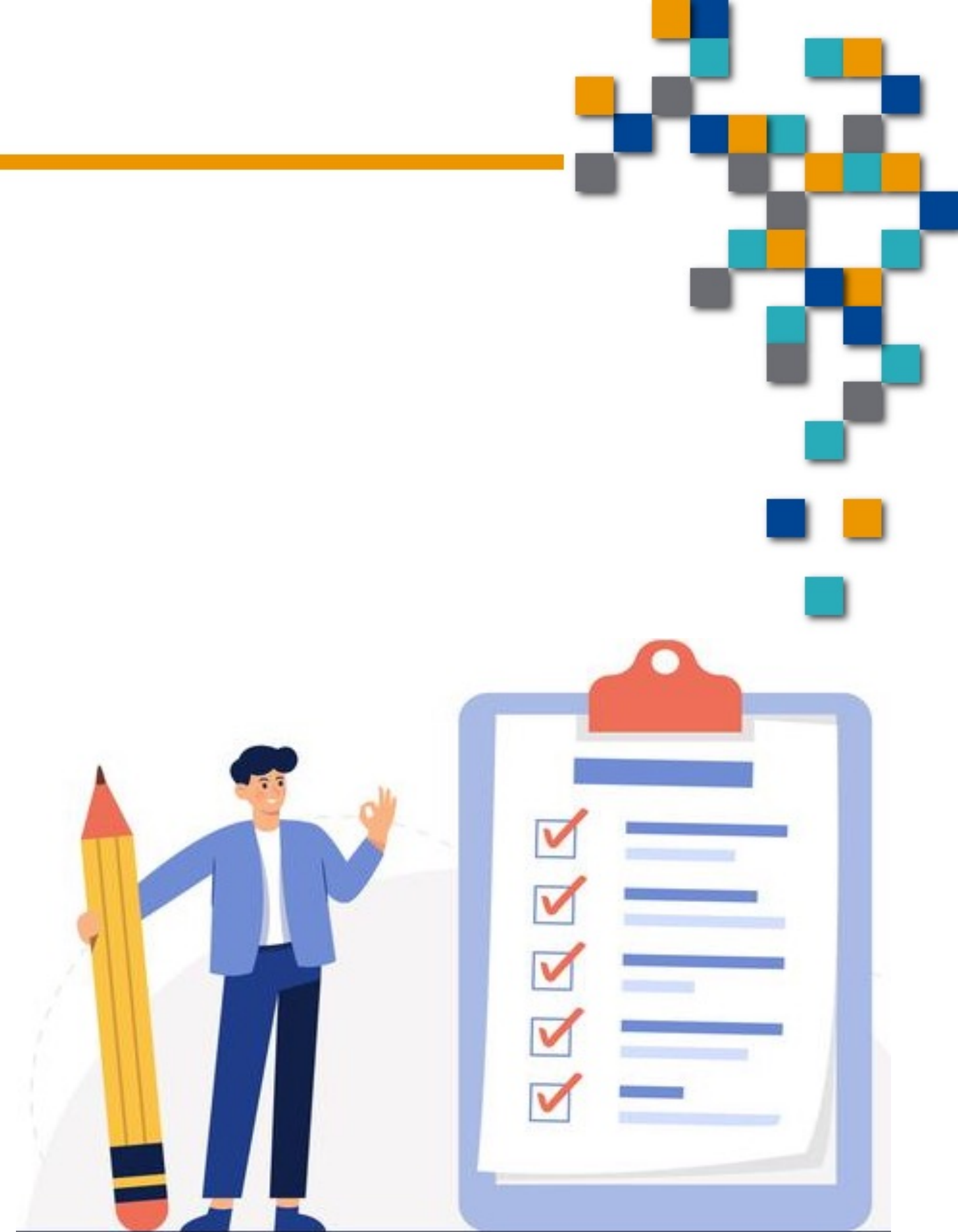


Introduction sécurité numérique



Sujets traités

- Découvrir les enjeux de nos informations en ligne
- Reconnaître et se protéger de l'hameçonnage
- Découvrir la sécurité sur internet
- Protéger son ordinateur
- Créer un mot de passe sécurisé
- Quiz



Vols d'identité dans l'actualité

Avis aux membres Desjardins – Renseignements personnels

Pour bien protéger ses membres, le Mouvement Desjardins désire assurer un suivi en lien avec l'annonce concernant la fuite de renseignements personnels.

Voici de nouveaux éléments importants que nous souhaitons vous communiquer :

- Certains membres nous ont signalé les longs délais auxquels ils font face lors de l'activation du forfait de surveillance du crédit d'Equifax par téléphone. Nos équipes travaillent sans relâche afin de trouver des solutions qui réduiront ce temps d'attente. Nous avons confiance de pouvoir les mettre en place d'ici quelques jours.
- Dans la majorité des cas, cette activation est plus rapide en utilisant le site Web d'Equifax. Nous rappelons que le code pour activer le service de surveillance du crédit d'Equifax vous sera uniquement envoyé par la poste. Desjardins ne vous contactera ni par téléphone, ni par courriel, ni par message texte.
- Nous tenons à nouveau à rassurer nos membres que, comme toujours, leurs actifs et transactions chez Desjardins sont protégés. Les membres ne subiront aucune perte financière si des transactions non autorisées sont réalisées dans leurs comptes Desjardins à la suite de cette situation.

Desjardins vous offre également un service d'assistance advenant un vol de

FAITS DIVERS

Fuite de renseignements personnels chez Revenu Québec



LA PRESSE+

TWITTER

Des données personnelles utilisées sans consentement

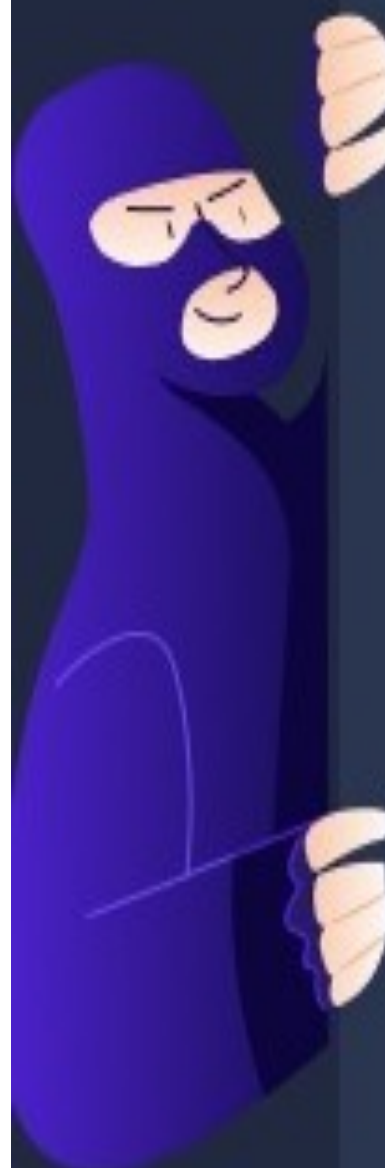
Twitter a annoncé hier que des données personnelles de ses utilisateurs avaient été utilisées à des fins publicitaires depuis mai 2018 sans leur consentement explicite. Le réseau social précise que l'erreur a été corrigée lundi et qu'une enquête est en cours pour déterminer combien d'utilisateurs ont pu être concernés, conseillant au passage à ces derniers de revoir leurs réglages en matière de partage des données. Selon Twitter, cela concerne deux cas de figure particuliers : si un utilisateur a regardé sur une publicité pour une application mobile ou cliqué sur celle-ci, d'une part, ou en envoyant des publicités basées sur l'appareil utilisé pour se connecter au réseau, d'autre part. — AFP



Fuite massive de données chez Capital One

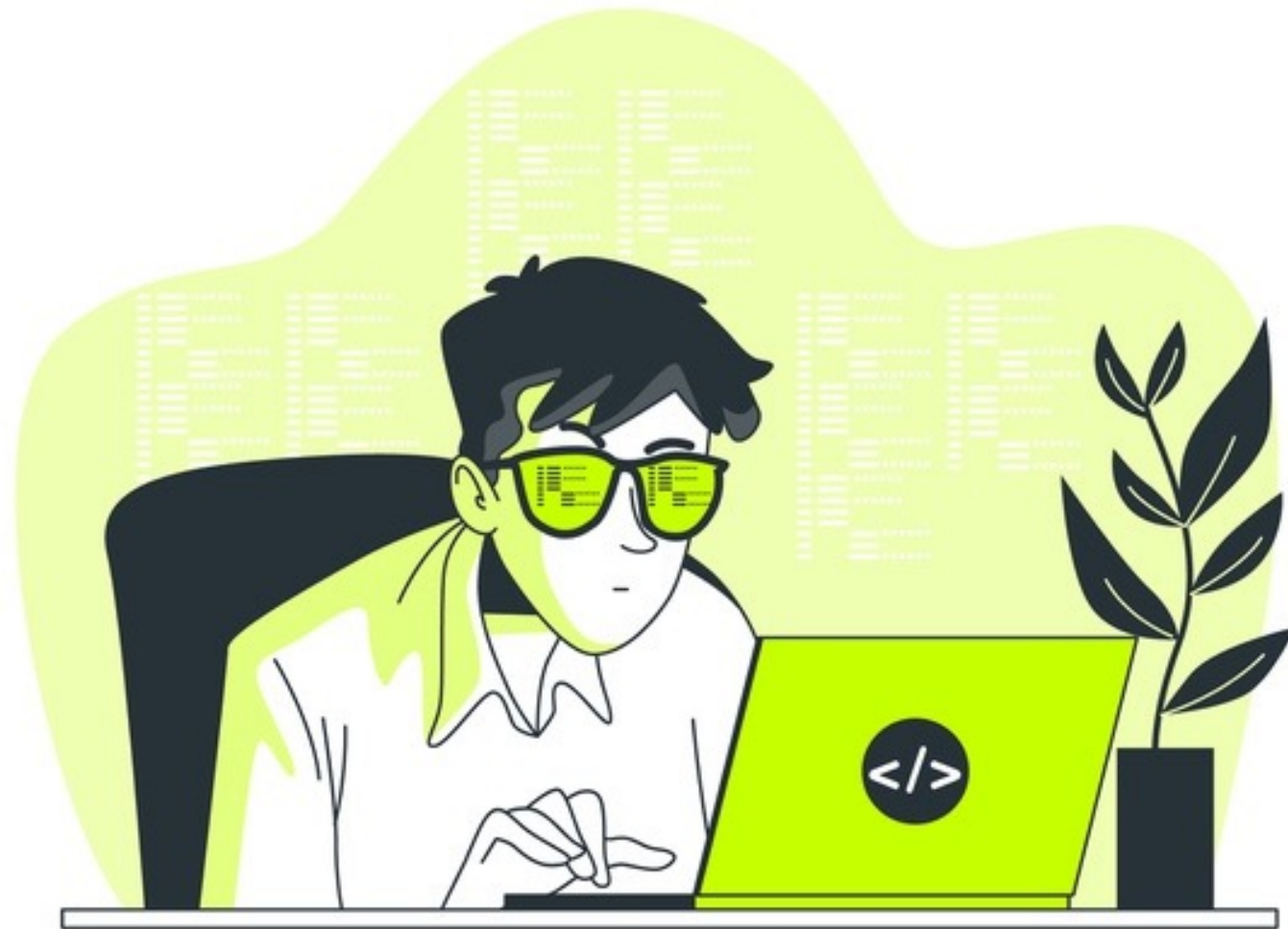
Près de 6 millions de clients canadiens touchés par le vol de données

Exemples d'arnaques sur le vaccin contre la Covid-19



- Tentatives de hameçonnage
L'arnaque le plus courant est celui de l'e-mail, d'apparence officielle, proposant un vaccin. Il suffit de remplir un formulaire avec ses données personnelles et bancaires... En fait, ces données sont volées et aucun vaccin n'est envoyé.
- Arnaques sur des e-boutiques
Ce type de scam s'est étendu aux vaccins. Vous payez le fournisseur mais vous ne recevez rien du tout. C'est pour cela que vous devez absolument acheter le vaccin depuis des sources réputées et surtout pas sur Internet.
- Usurpation d'identité
Les fraudeurs se font passer pour des organisations connues (prestataires de soins de santé, etc.) pour vous inspirer confiance et vous vendre des vaccins ou des tests. En fait, ils encaissent l'argent et disparaissent dans la nature.

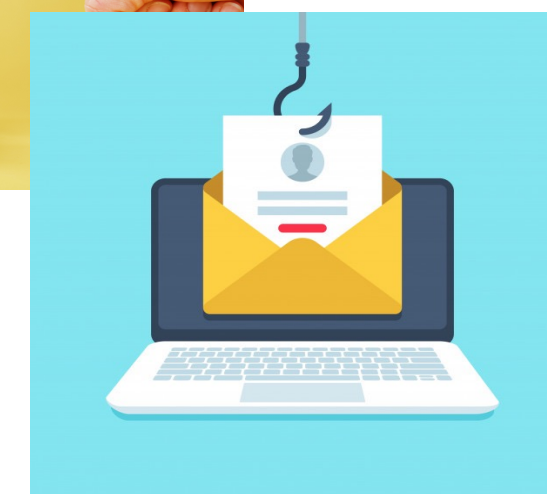
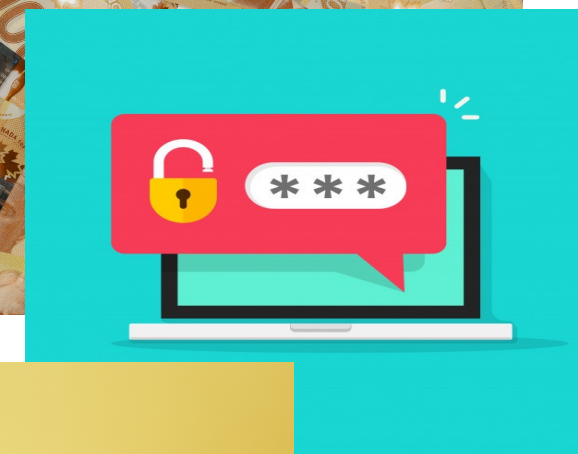
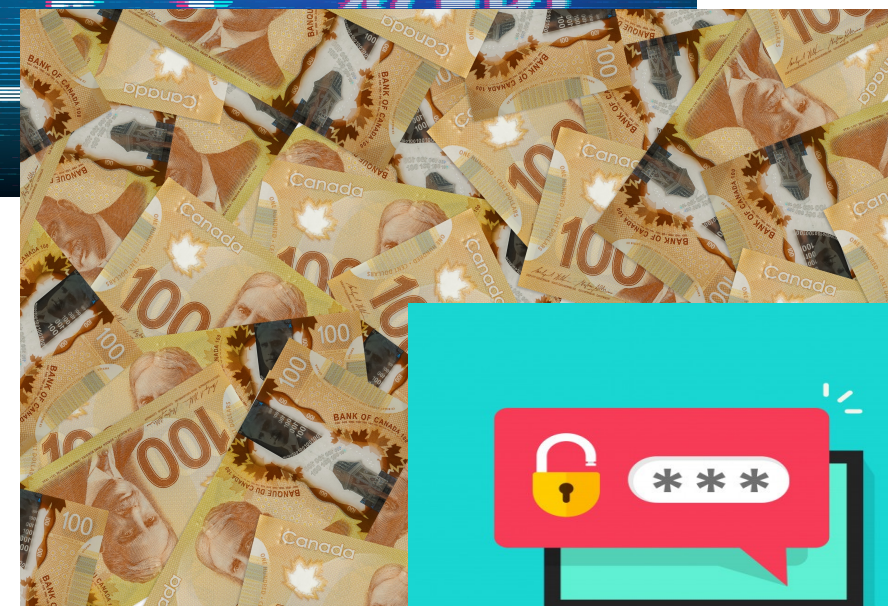
La différence entre un hacker et un pirate informatique



La **différence** notable **entre** ces deux pratiques **est** que le **hacker** aide à colmater ces failles tandis que le **pirate** cherche à les exploiter.

Quelles sont les techniques des pirates ?

- Installer un virus ou logiciel malveillant (Maliciel).
- Faire des propositions: "Trop beau pour être vrai".
- Exploiter des réseaux wifi non sécurisés.
- Exploiter des sites web non sécurisés.
- Envoyer des tentatives hameçonnage.



Qu'est-ce que des informations personnelles ?

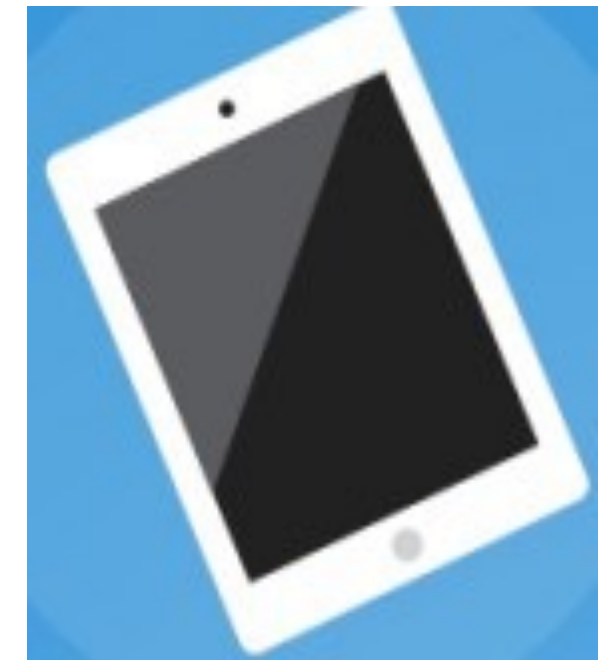
Toutes formes d'identification:

- No du permis de conduire
- No de sa carte d'assurance maladie
- No d'assurance sociale
- Carte de débit ou crédit
- Adresse et no de téléphone
- Date de naissance, sexe, ville
- Nom de (jeune fille) votre mère



Où laissez-vous vos informations sur Internet?

- Les réseaux sociaux
- Site Internet
- Moteur de recherche
- Formulaire en ligne
- Application mobile



Qui collecte vos informations ?

- Les applications
- Les logiciels
- Les sites web
- Les systèmes d'exploitation



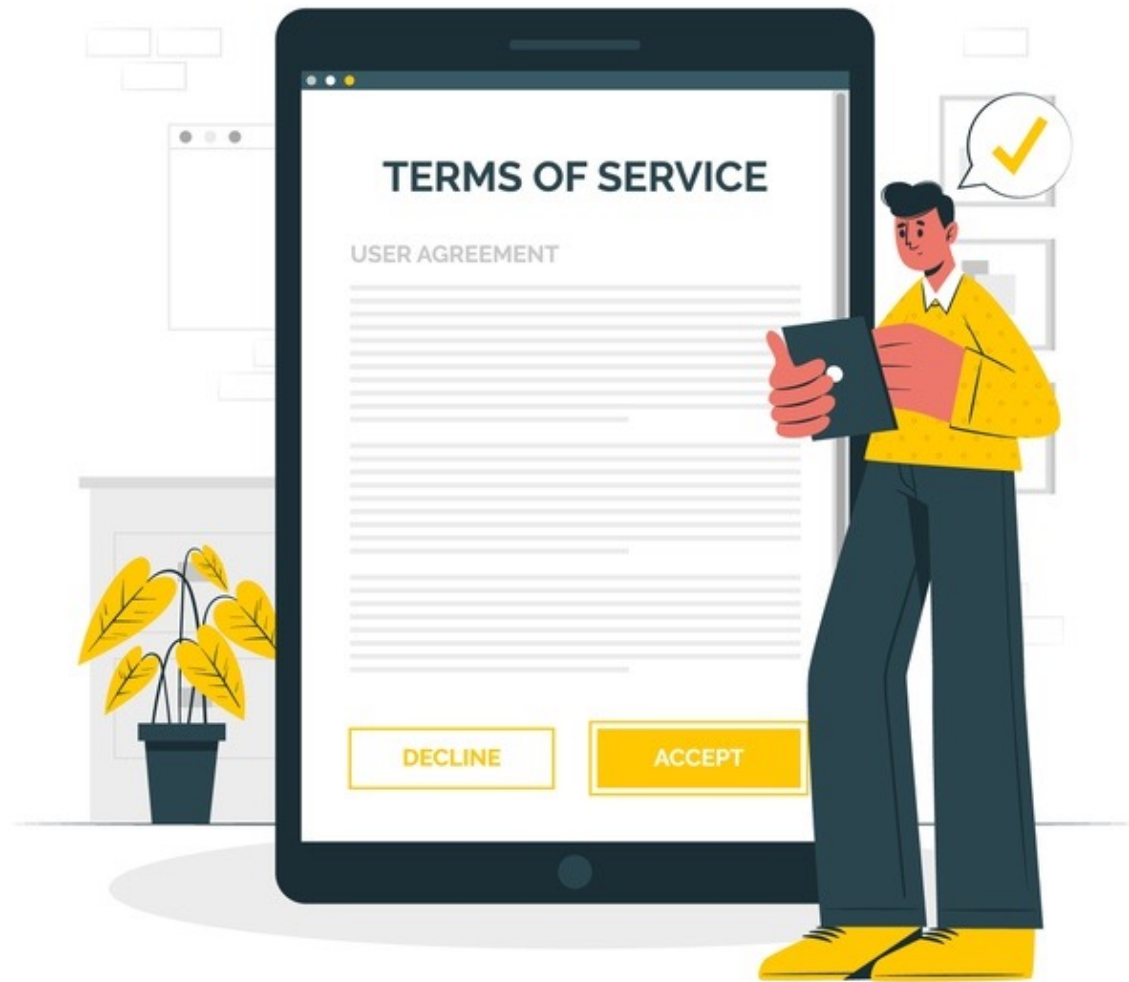
Pourquoi ces entreprises veulent vos informations?



- Permet aux entreprises de vous identifier.
- Permet aux entreprises à vous afficher des produits.
- Permet aux entreprises d'afficher des publicités ciblées.



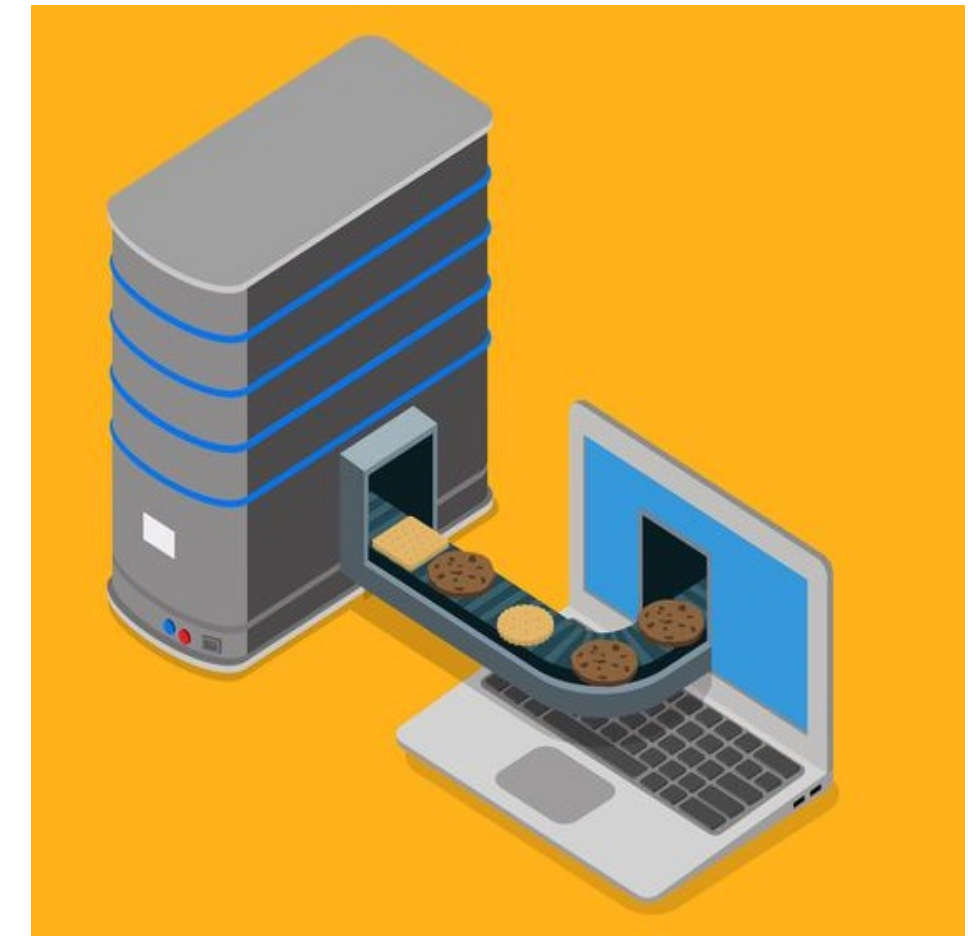
Comment les entreprises collectent-elles vos données?



**Conditions
d'utilisation**



**Comportement
en ligne**



**Témoins de
navigation**

Conseil pour protéger ses informations personnelles

- Refuser les témoins (cookies).
- Paramétrer son navigateur.
- Choisir un moteur de recherche sécurisé.
- Le choix de ne pas tout divulguer.
- Lire les conditions de l'entreprise.





Reconnaître et se
protéger de
l'hameçonnage

Qu'est-ce-que l'hameçonnage?

L'hameçonnage est une tentative faite par des cybercriminels pour s'emparer de vos renseignements personnels, par différent moyens, en prétendant être un expéditeur légitime.



Les différentes formes d'hameçonnage



L'hameçonnage par message texte utilise le message texte comme outil.



L'harponnage

est une tentative extrêmement ciblée conçue pour ressembler à un message provenant d'une source que vous connaissez.

Les différentes formes d'hameçonnage



La mystification

consiste à créer un faux site web dans le but d'inciter une personne à révéler ses renseignements personnels.



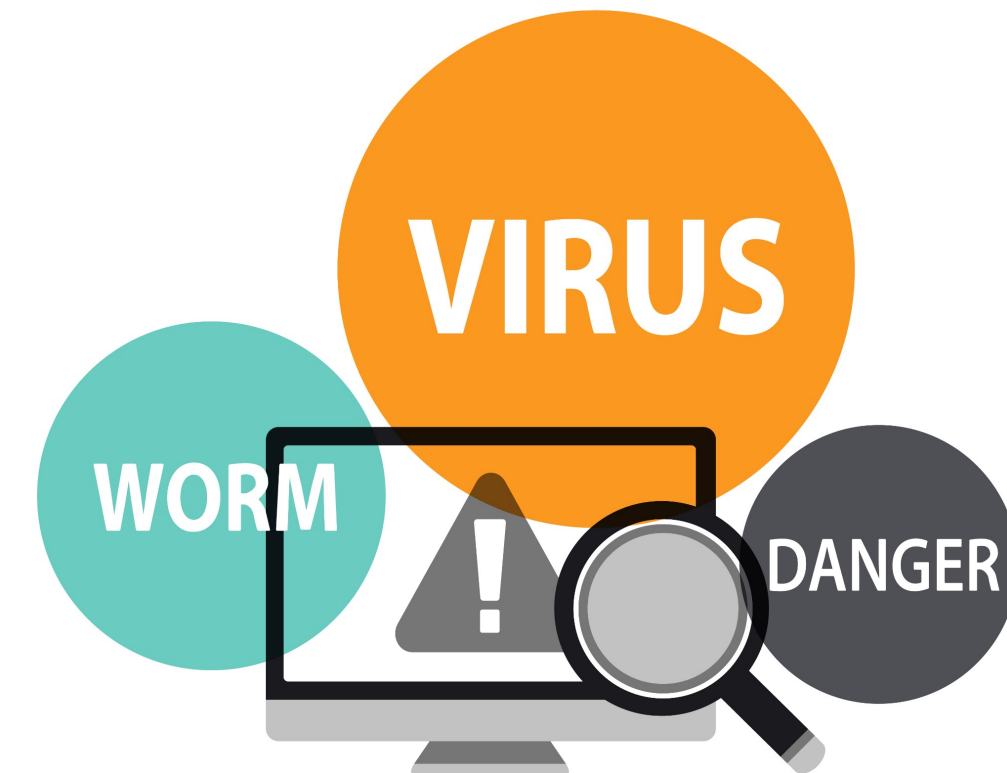
La chasse à la baleine (ou le *whaling*)

est une forme d'hameçonnage ciblant des personnes importantes comme un haut dirigeant d'entreprise ou un supérieur dans une organisation ou un ministère.

Qu'est-ce qu'un maliciel ?

Les maliciels sont des logiciels malveillants comme par exemple:

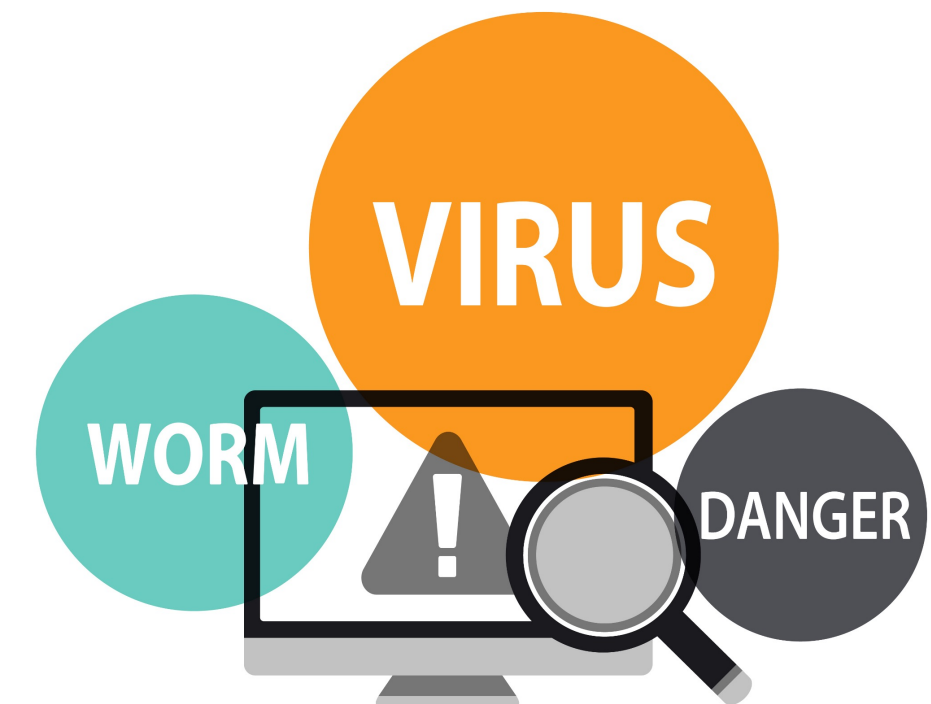
- Des virus
- Des logiciels espions
- Des applications malveillantes
- Des scarewares



Qu'est-ce qu'un maliciel (suite)?

Si votre appareil a été infecté par un maliciel, certains des symptômes suivants pourraient apparaître :

- **Ordinateur plus lent**
- **Difficultés à accéder l'Internet**
- **Des paramètres modifiés**
- **Usage de donnée Internet plus élevé**
- **Des applications inconnues**



Notre vulnérabilité en ligne

- Courriel
- Médias sociaux
- Site web
- Appareil intelligent





**Pression ou langage
menaçant**

Les signaux d'un message d'hameçonnage

MÉFIEZ-VOUS :



- Des messages qui insistent pour que vous répondiez rapidement.
- Des messages qui menacent de fermer votre compte ou d'intenter des poursuites.



INFORMATIONS SENSIBLES DEMANDÉES

Les signaux d'un message d'hameçonnage

MÉFIEZ-VOUS :

- Des liens vers des pages d'ouverture de session
- Des demandes de renseignements financiers, même s'ils semblent provenir de votre banque
- Des demandes de mise à jour des renseignements associés à vos comptes





**TROP BEAU POUR
ÊTRE VRAI**

Les signaux d'un message d'hameçonnage

MÉFIEZ-VOUS :

- Des prix gagnés dans le cadre d'un concours auquel vous n'avez jamais participé
- Des prix pour lesquels vous devez payer des frais
- De l'héritage d'un membre de la famille éloignée





Courriels inattendus

Les signaux d'un message d'hameçonnage

MÉFIEZ-VOUS :



- Des reçus pour des articles que vous n'avez pas commandés
- Des suivis d'envoi pour des articles que vous n'avez pas commandés



RENSEIGNEMENTS DOUTEUX

Les signaux d'un message d'hameçonnage

MÉFIEZ-VOUS :



- Des courriels provenant d'adresse incorrecte (mais parfois semblable à une adresse légitime)
- Des liens qui ne mènent pas à un site officiel
- Des erreurs d'orthographe ou de grammaire



PIÈCES JOINTES SUSPECTES

Les signaux d'un message d'hameçonnage

MÉFIEZ-VOUS :

- Des pièces jointes que vous n'avez pas demandées
- Des noms de fichiers bizarres
- Des types de fichiers inhabituels





GRAPHISME AMATEUR

Les signaux d'un message d'hameçonnage

MÉFIEZ-VOUS :



- Des logos inexacts ou flous
- Des courriels ne contenant que des images
- Des courriels d'entreprises mal mis en page

Les signaux d'un message d'hameçonnage

**SI VOUS REPÉREZ L'UN DE CES
SIGNAUX D'ALARME
DANS UN MESSAGE :**



ne cliquez
sur aucun lien



ne répondez
pas et ne le
transférez pas



n'ouvrez
pas les
pièces jointes



**SUPPRIMEZ LE COURRIEL OU LE TEXTO,
OU, EN CAS DE DOUTE, TENTEZ DE REJOINDRE
L'EXPÉDITEUR PAR UN AUTRE MOYEN.**

Le processus d'un hameçonnage par courriel



1

Vous recevez un message qui semble venir d'un proche ou d'une entreprise que vous connaissez.

2

On vous demande de répondre en toute urgence en cliquant sur un lien ou une pièce jointe.

3

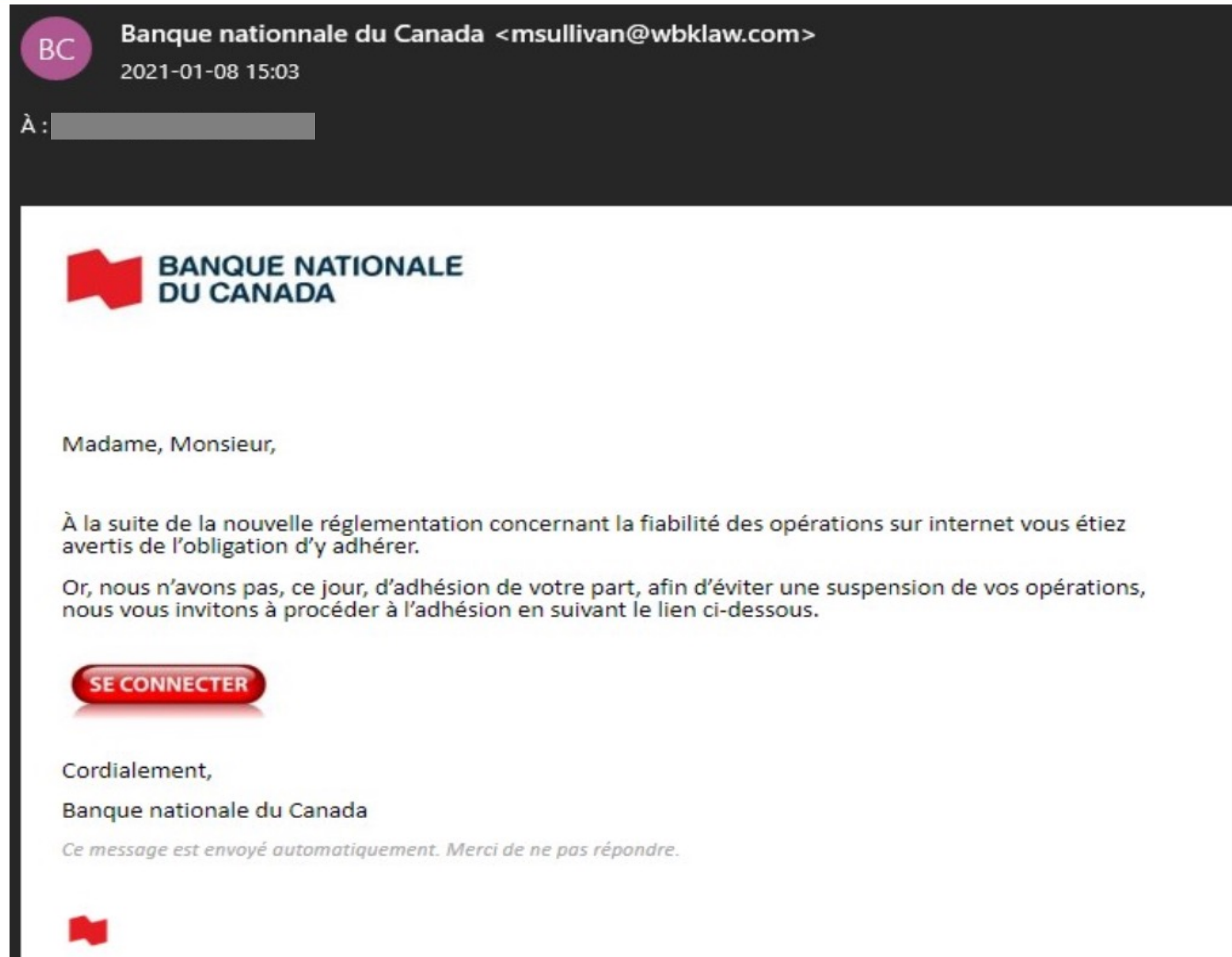
On vous demande des informations personnelles par message ou par un formulaire en ligne.

4

Les pirates informatiques utiliseront ces informations sans votre autorisation.

Exemple d'hameçonnage par courriel

Pour mettre à jour vos informations ou pour vous connecter au compte de votre banque, allez sur le site Internet officiel!

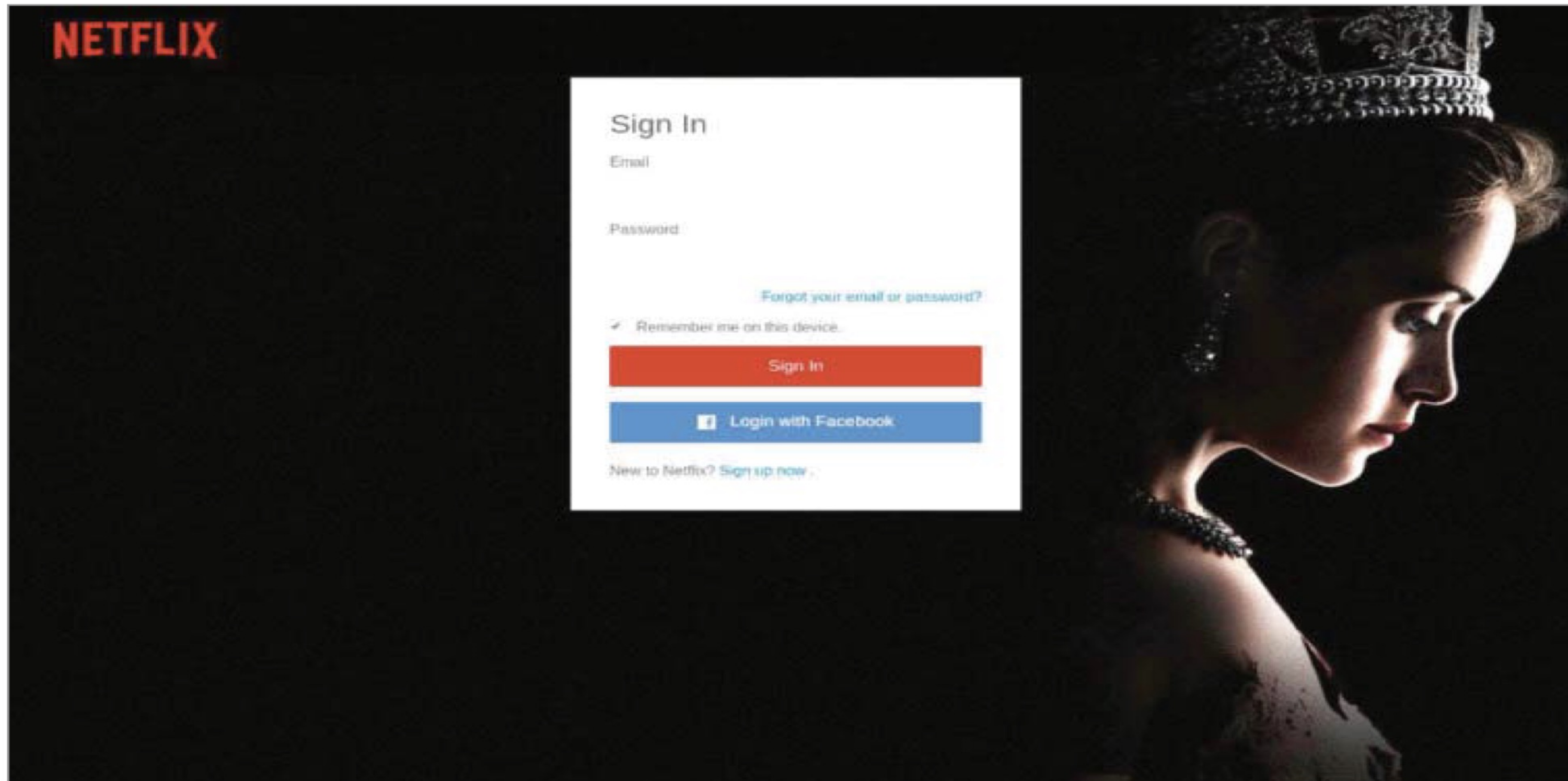


Comment reconnaître un site Web frauduleux ?



- Adresse différente
- Logos utilisés différents des logos officiels
- Peut contenir des fautes d'orthographe et de grammaire.
- Mise en page simpliste
- Utilisation de formules générales pour se donner de la crédibilité
- Polices et couleurs d'écriture non uniformes

Exemple d'un site hameçonnage(Netflix)



DR

Cette fausse page de connexion à Netflix – accessible via un lien intégré aux courriels de phishing apparus pendant les fêtes de Noël – n’était simplement pas hébergée sur les serveurs du service. Il est préférable d’utiliser l’adresse du site web en la remplissant de votre main.

Exemple d'un site hameçonnage(Netflix)



No-reply

Service cancelation : reactivate your service

À : Pierre Wolfshagen

Boîte de réception - Videotron 07:45

NETFLIX

Update your payment details

Hello,

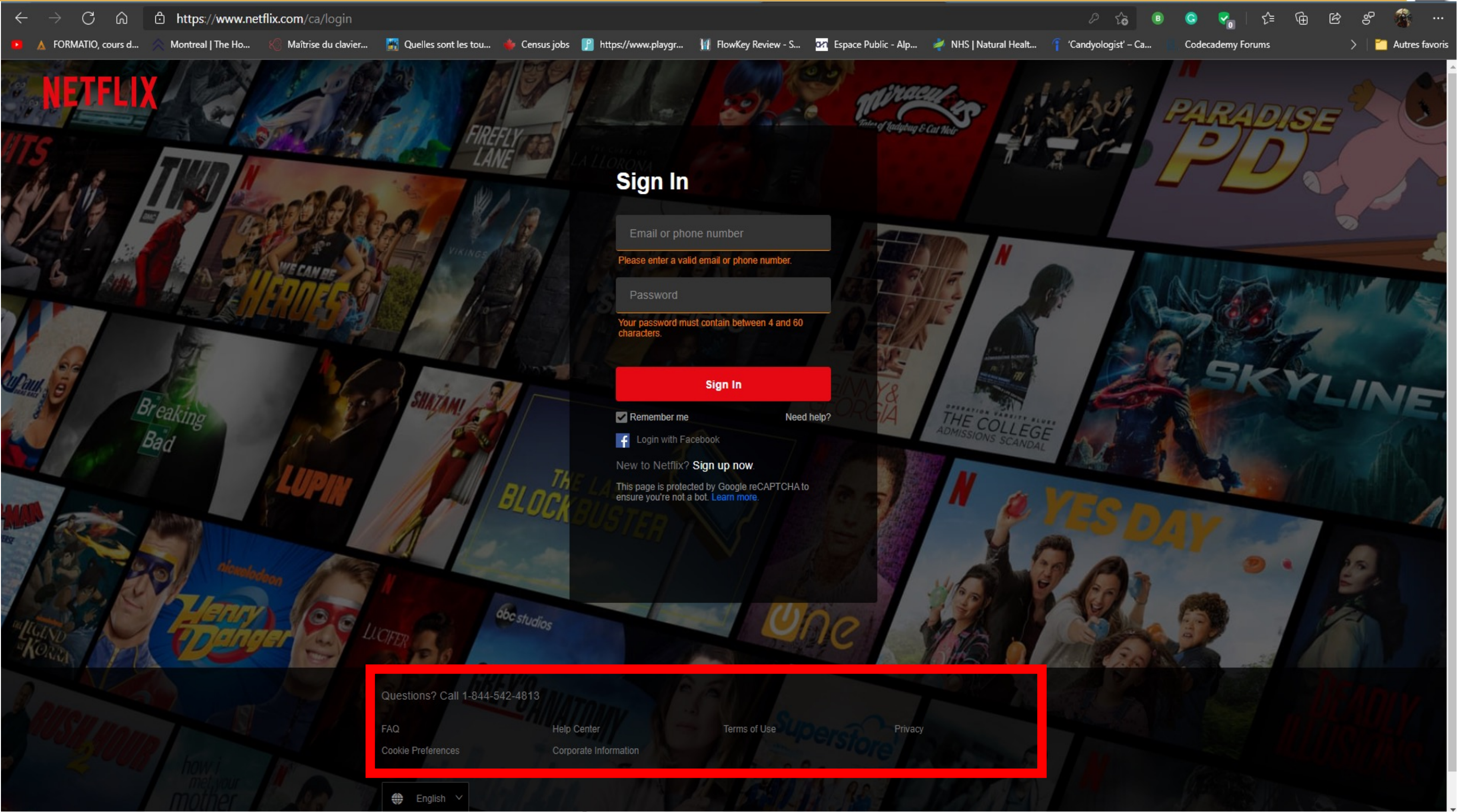
We are having problems with your current billing information. We will try again, but in the meantime, you may want to update your payment details.

UPDATE ACCOUNT

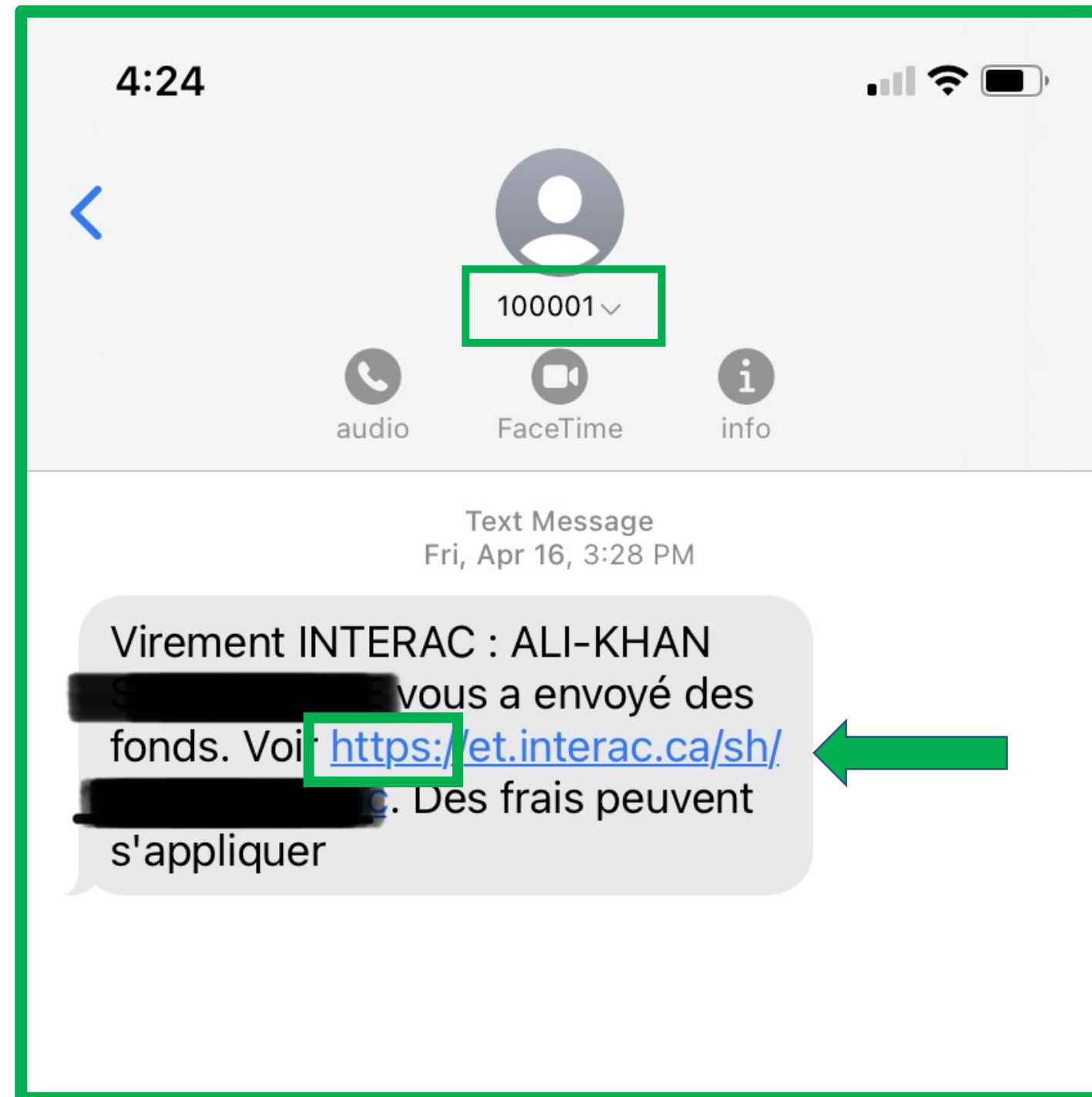
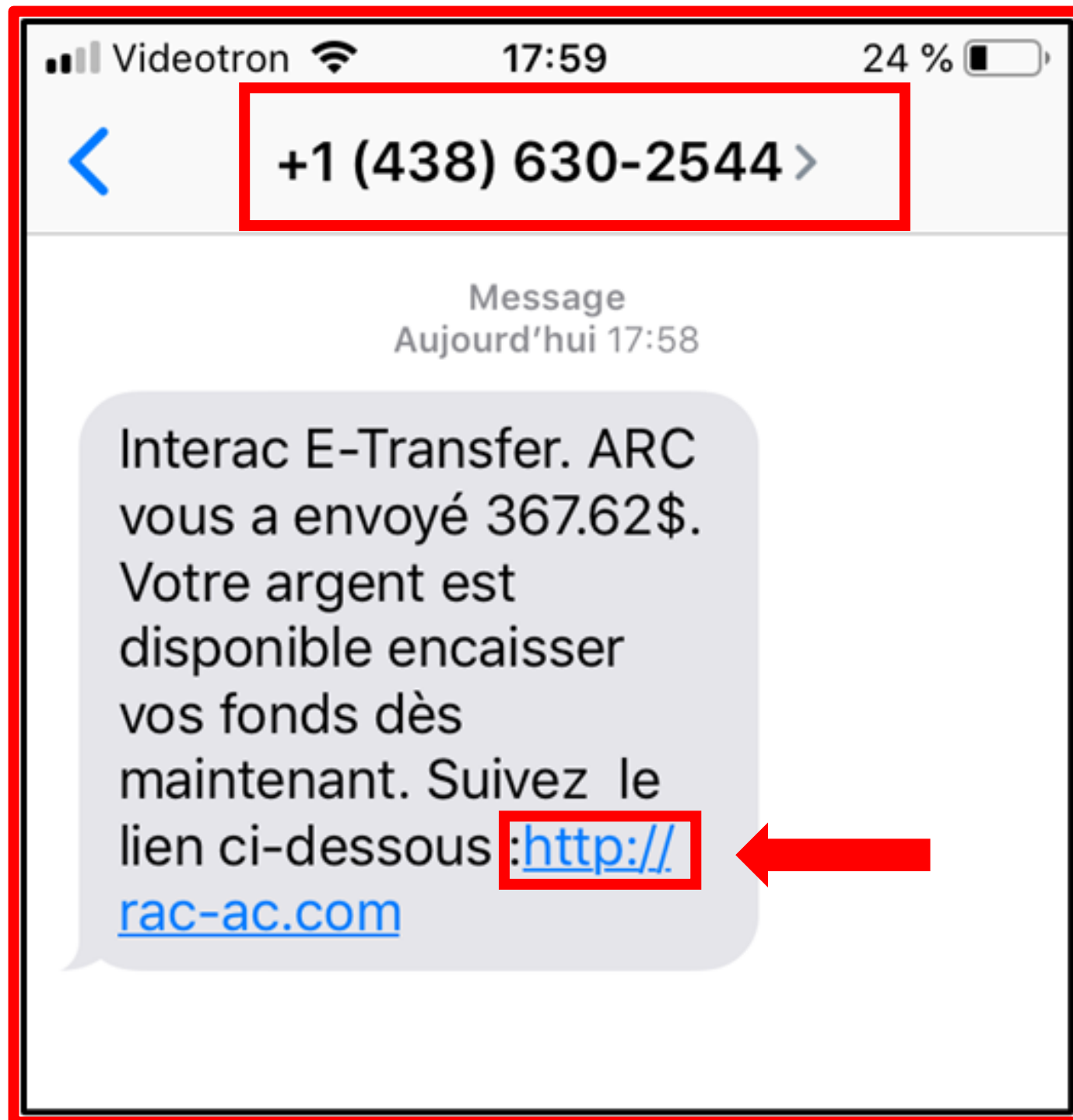
Need help? We are here if you need it. Visit the Help Center or contact us now.

–Your friends on Netflix

Exemple du site web officiel de Netflix



Exemple d'un hameçonnage par texto



Exemple d'un hameçonnage par texto

mosaïque57@hotmail.com

À : +1 (989) 408-8984

Message
Aujourd'hui 12:17

Votre accès en ligne de
Banque Nationale est
désactivé. Veuillez remplir le
formulaire ci-dessous.

<https://bnc09reset.com/1>



mosaïque57@hotmail.com



2590-payments-interac-cra

4538 - Virement INTERAC : Obtenir un remboursement 1/16/2022 - 023240

À : Pierre Wolfshagen

Virement/INTERAC e-Transfer

Bonjour wolfshagen@videotron.ca,
Vous avez reçu 458.00\$ CAD de C R A

[\[Obtenir un remboursement\]](#)

Expire le: 1/17/2021

Exemple d'hameçonnage par réseaux sociaux



2018COUPONS.WIN

Costco is giving Free \$75 Coupon Per family to celebrate its 50th Anniversary!

Que faire si vous avez cliqué sur un lien d'un message frauduleux?

Si vous n'avez pas fourni d'informations personnelles

- En premier lieu, changer vos mots de passe de tous les sites qui utilisent les mêmes mots de passe que le site web frauduleux.

Si vous avez fourni des informations confidentielles ou financières.

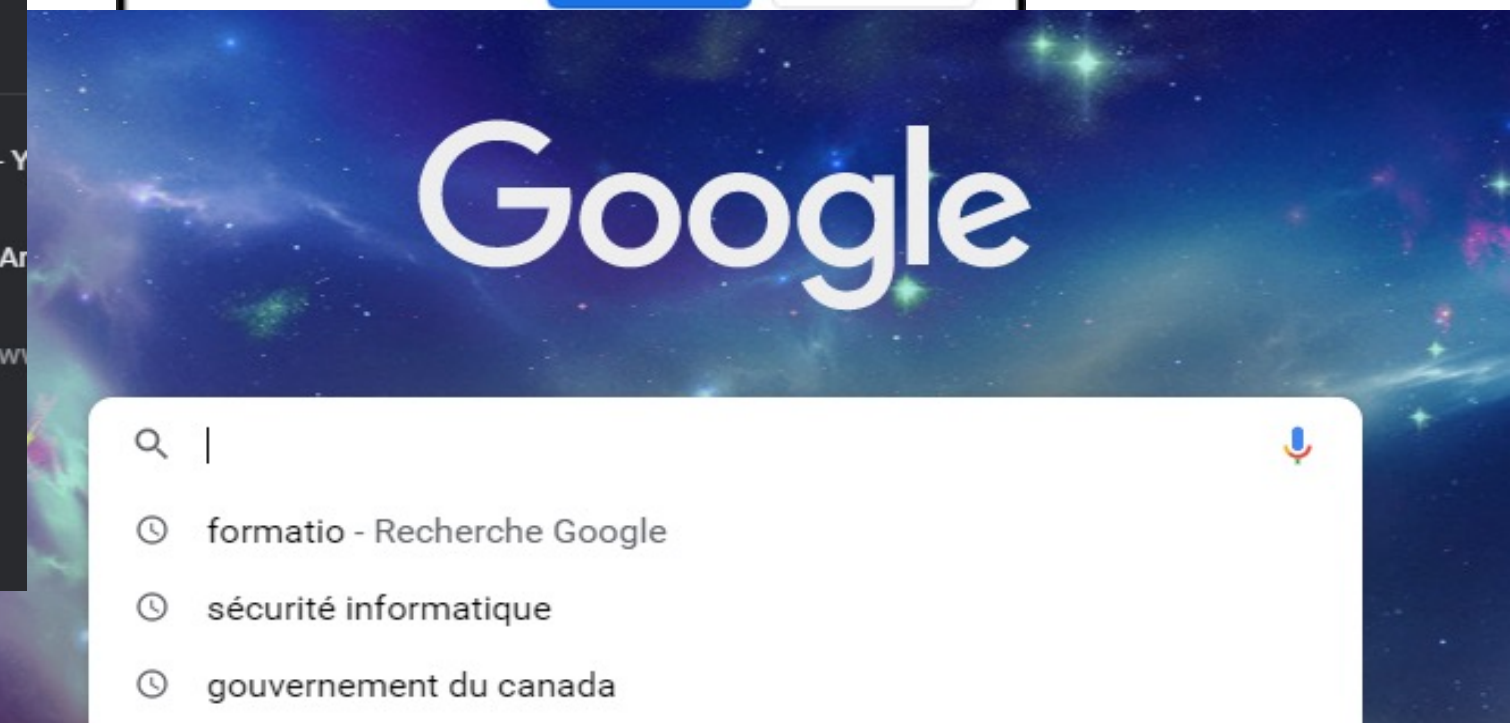
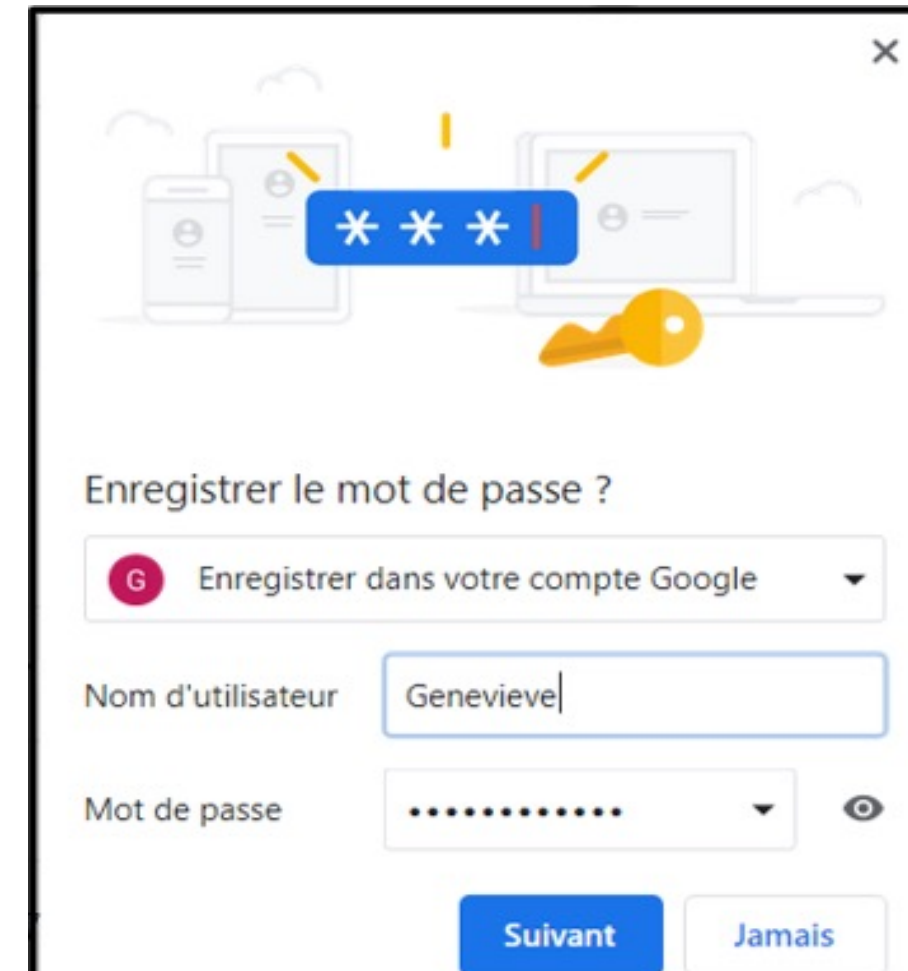
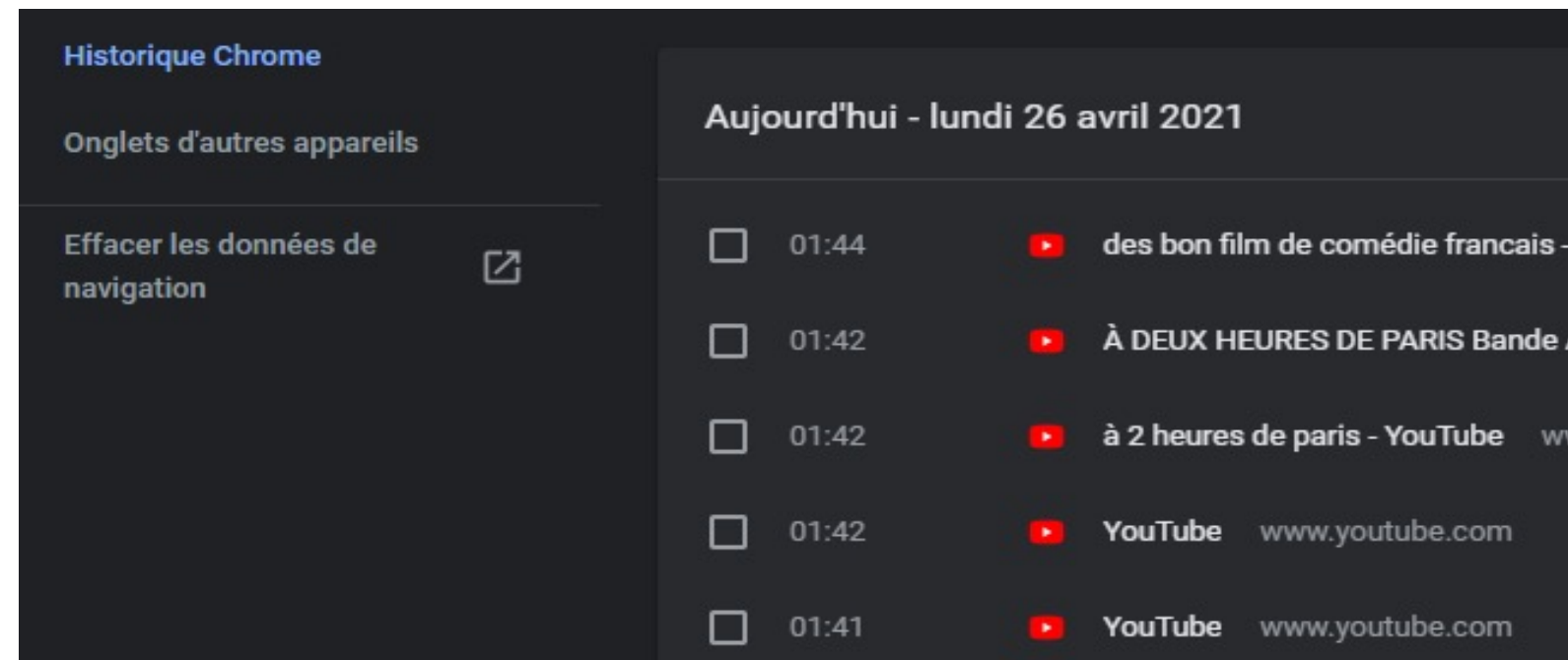
- Faire un rapport à la police locale.
- Contacter et informer votre banque.
- Aviser les agences de crédit pour qu'elles ajoutent une note à votre dossier afin d'informer les fournisseurs de crédit.
- Aviser le centre antifraude du Canada



La sécurité sur internet

Quelles sont les informations enregistrées par un navigateur?

- Les sujets de recherches
- Les sites Web visités
- Les identifiants et mots de passe

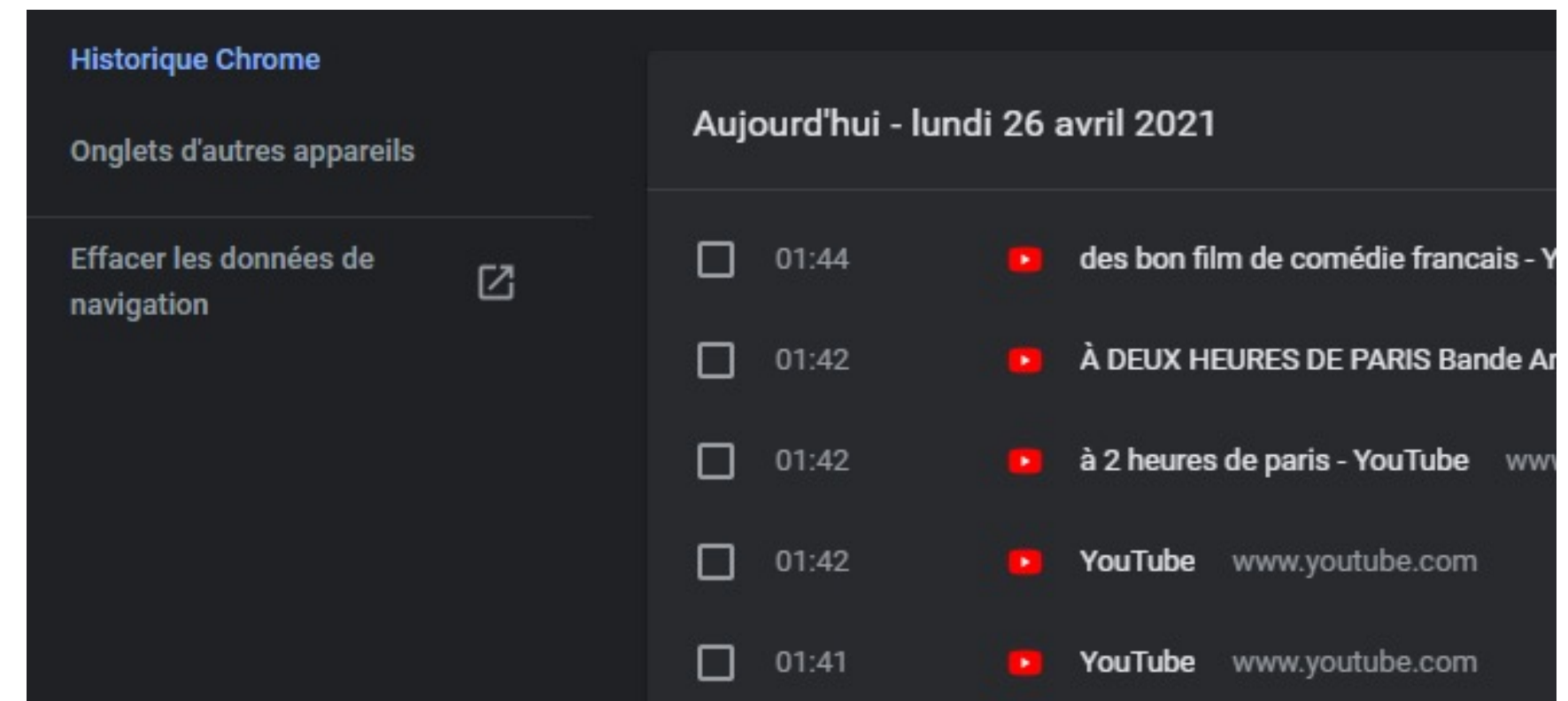


Qu'est-ce qu'un historique de navigation ?



L'historique de navigation contient:

- Le nom de la page web et l'URL
- L'heure et la date
- L'enregistrement chronologique

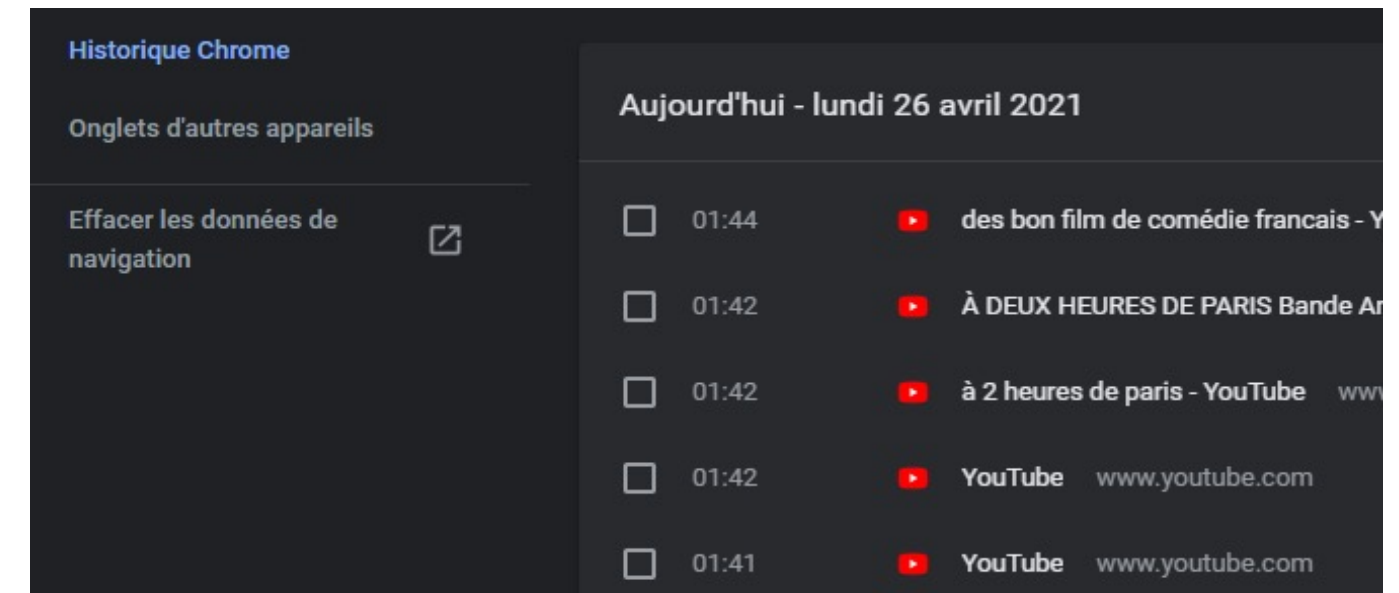


Qu'est-ce qu'un historique de navigation ?



L'historique de navigation permet:

- De pouvoir utiliser les boutons de navigation.
- De pouvoir revenir immédiatement sur une page antérieurement accédée.
- De pouvoir retrouver un site visité auparavant.



Qu'est-ce qu'un témoin (cookie)?

Les témoins de navigation permettent:

- Retenir les identifiants de connexion (identifiant et mot de passe)
- Stocker les paramètres d'affichage d'un site web
- Analyser les pages visitées



Les avantages de l'enregistrement en ligne?

- Permet d'obtenir des résultats de recherche plus précis, basés sur votre adresse IP.
- Permet de se connecter au compte avec un simple clic.
- Permet d'avoir une liste des activités récentes dans votre compte.

Naviguer en mode privé

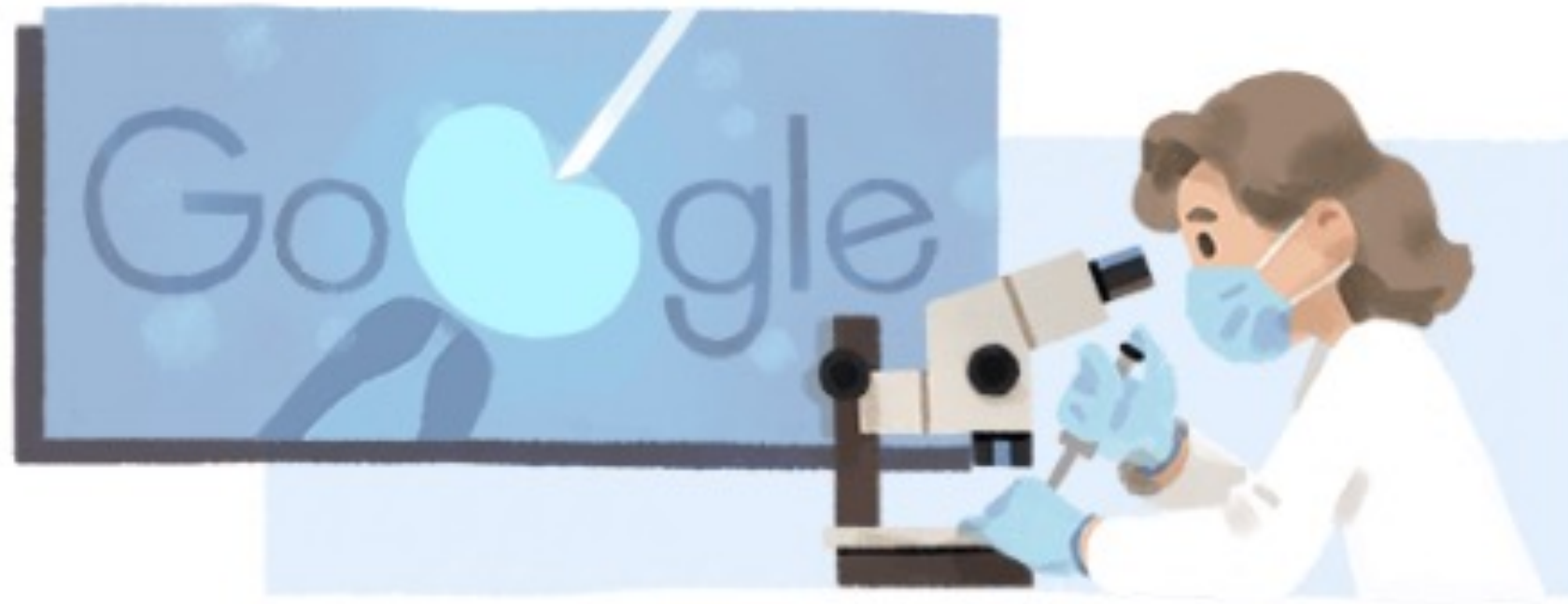


Les informations suivantes ne seront pas enregistrées :

- **Votre historique de navigation**
- **Les cookies et les données des sites visités**
- **Les informations saisies dans les formulaires**
- **Les mots de passe**
- **La liste des téléchargements**



Bien choisir son moteur de recherche



Recherche Google

J'ai de la chance

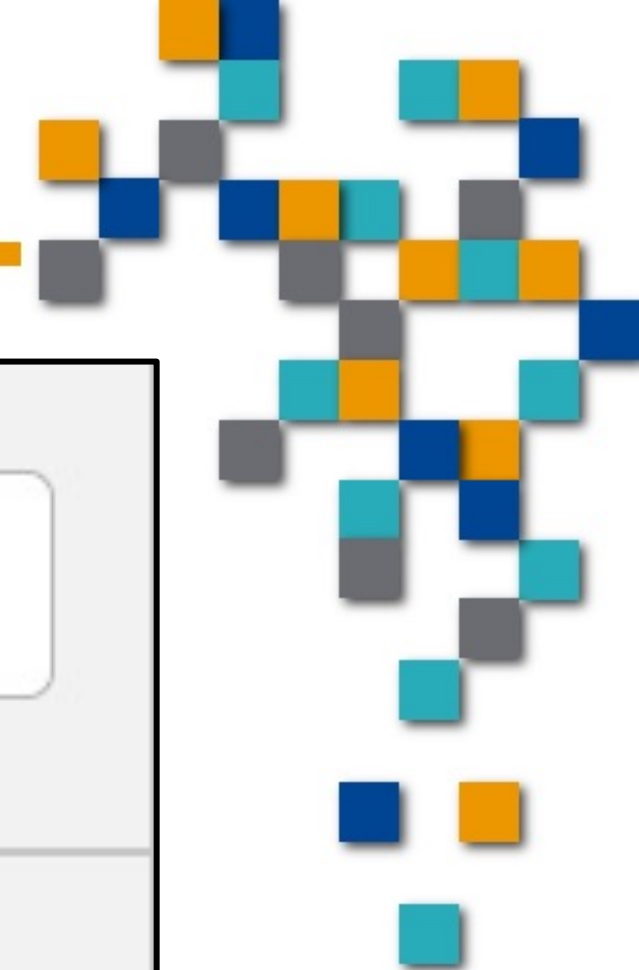
Google offert en : [English](#)

Bien choisir son moteur de recherche



VOUS AVEZ L'OPTION!

L'importance de https



Sécurisé



https://www.google.com

Non sécurisé



www.example.com

HTTP*



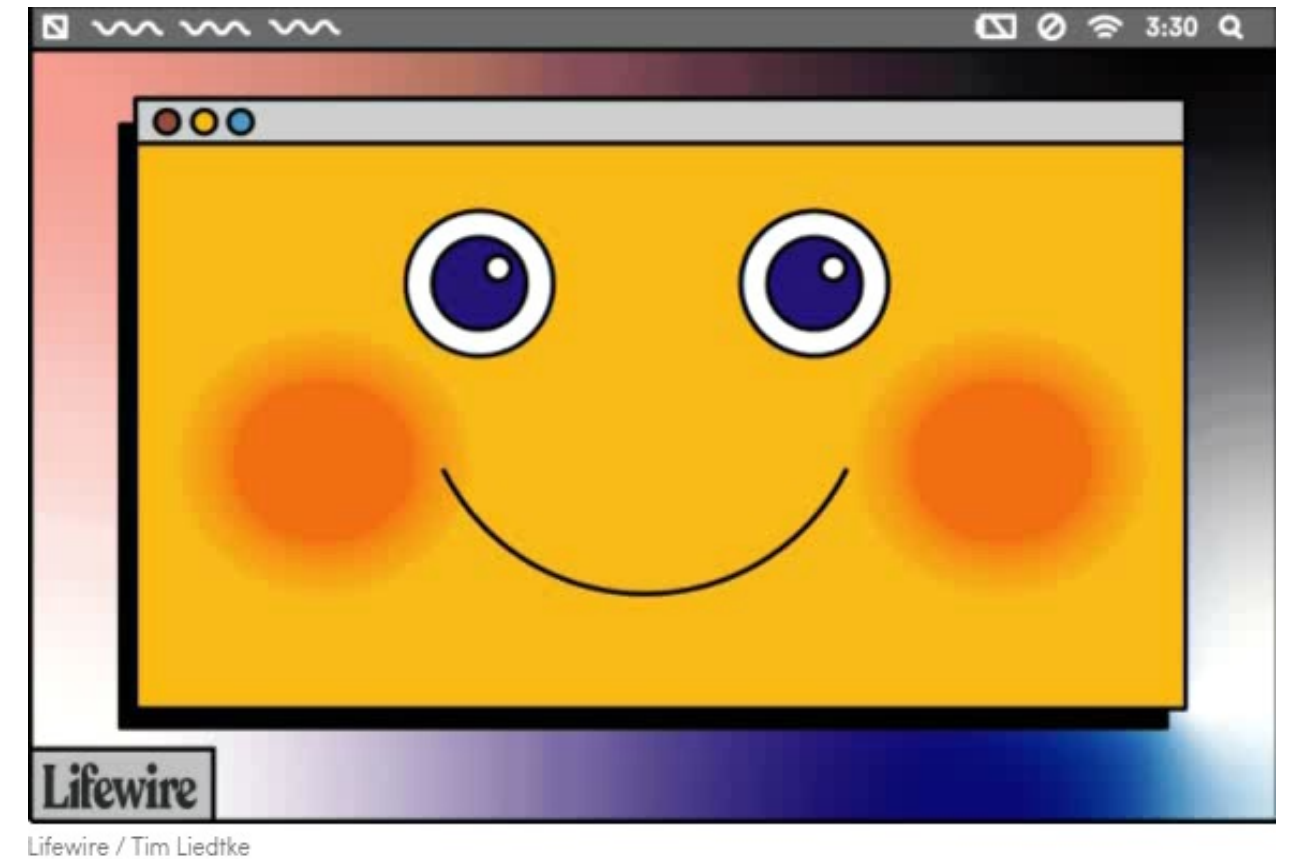
Non
sécurisé

example.com

Vider la mémoire

Les avantages:

- Permet de se protéger des maliciels.
- Aide à protéger votre ordinateur.
- Libère de l'espace sur votre disque dur.
- Force votre navigateur à récupérer la dernière copie disponible sur le site Web.



Vider la mémoire

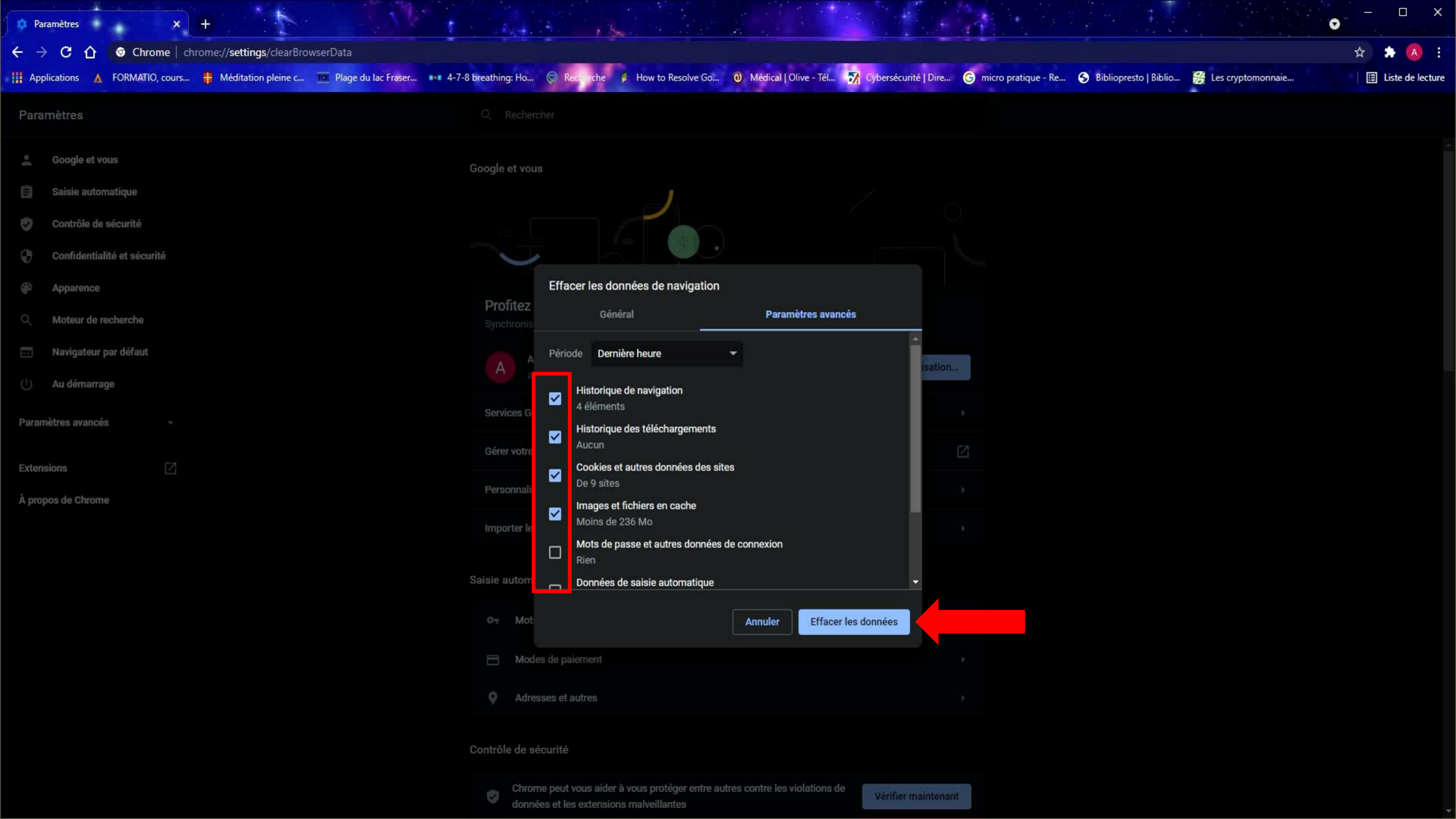
Windows:

- **Ctrl+Shift+Del**
- **Ctrl+Maj+Suppr**

Mac:

Commande+Maj+Suppr
Command+Shift+Delete





Effacer les données de navigation

Général

Paramètres avancés

Période Dernière heure

- ☒ Historique de navigation
4 éléments
- ☒ Historique des téléchargements
Aucun
- ☒ Cookies et autres données des sites
De 9 sites
- ☒ Images et fichiers en cache
Moins de 236 Mo
- ☐ Mots de passe et autres données de connexion
Rien
- ☐ Données de saisie automatique

Annuler

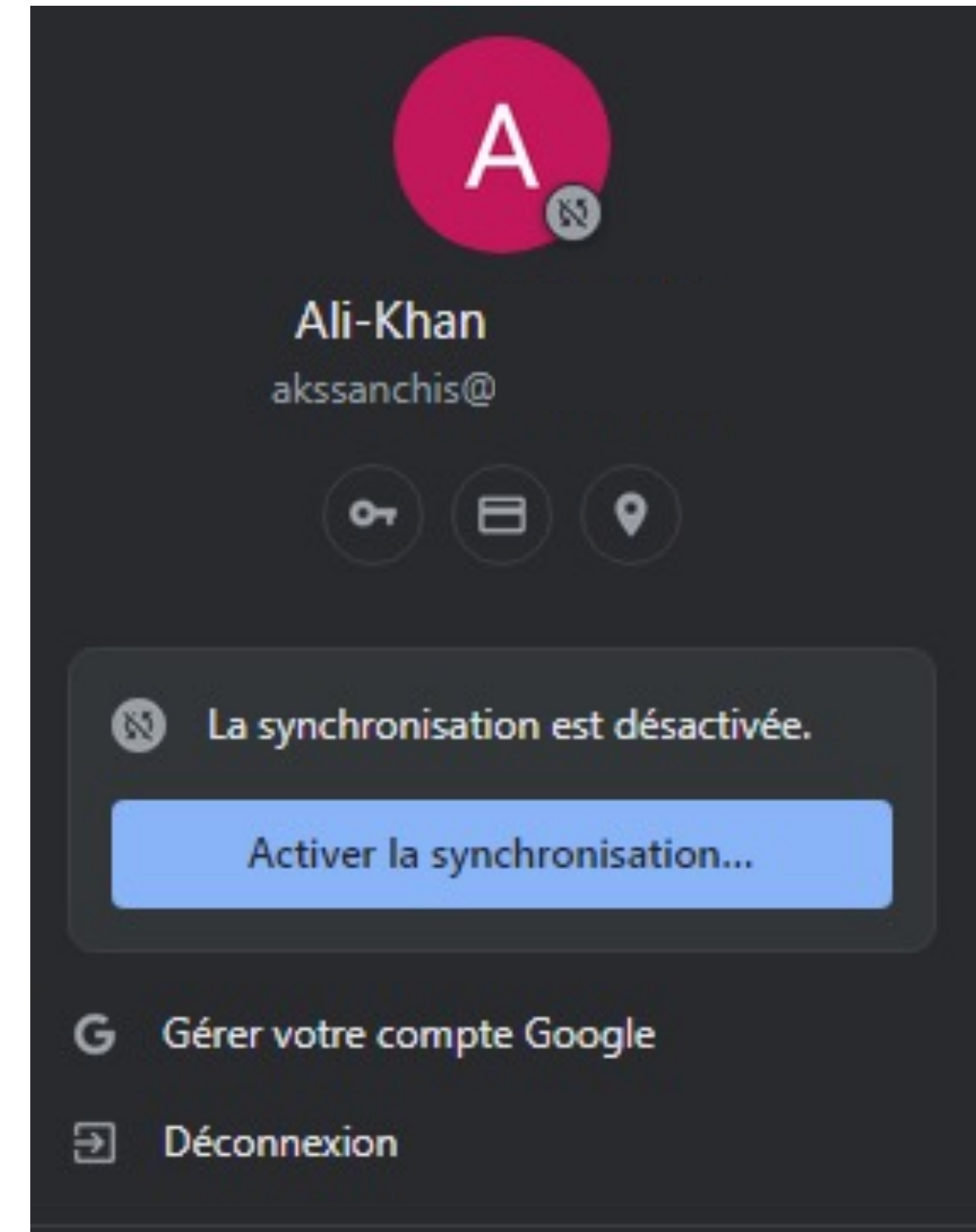
Effacer les données

Reconnaître les sites sécurisés



Conseil pour naviguer sur Internet

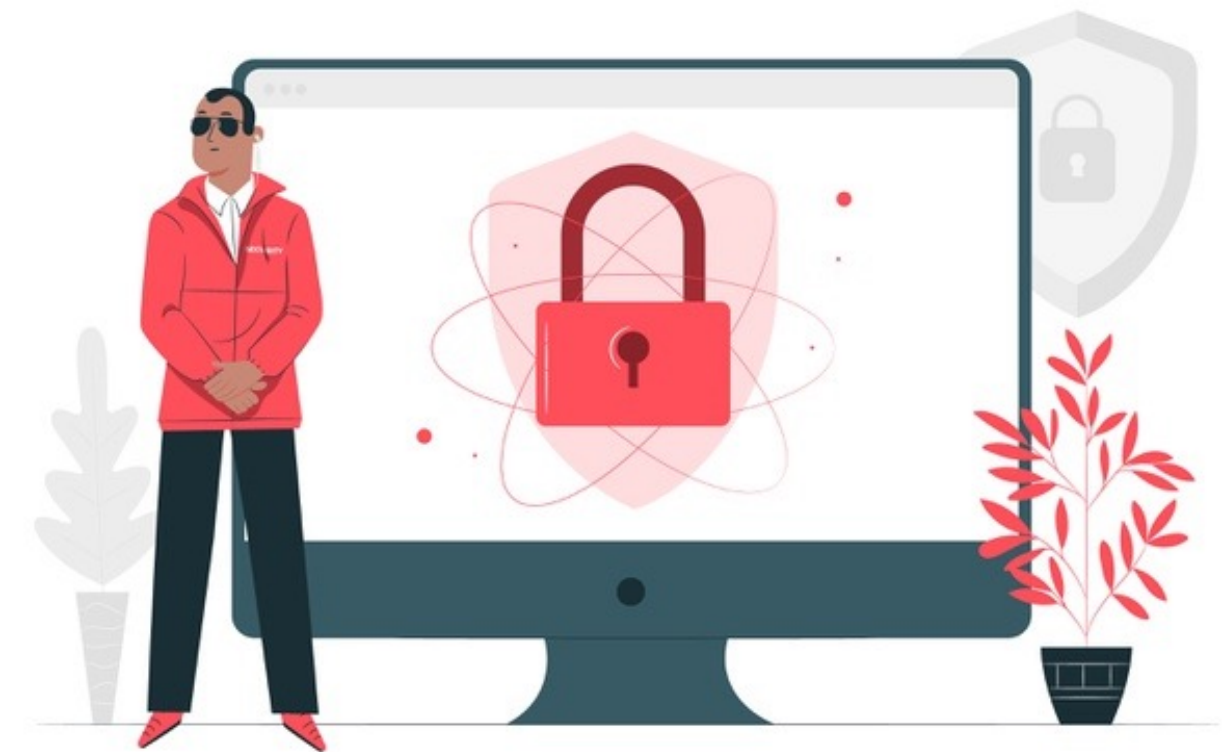
**Se déconnecter
de ses comptes
en ligne.**



Conseil pour naviguer sur Internet

Utiliser des mots de passe sécurisés

- Utiliser des mots de passe uniques.
- Avoir un mélange de lettres, chiffres et caractères spéciaux.
- Aucune information personnelle comme mot de passe.





Prudence avec les réseaux wifi publiques

- Éviter de faire des achats en ligne.
- Éviter de partager des informations personnelles.



Des bonnes pratiques sur les réseaux sociaux

Le droit de ne pas tout partager

Vous n'êtes pas obligés de fournir:

- **Votre nom**
- **Votre date de naissance**
- **Votre courriel principal**
- **Votre ville**
- **etc...**



La différence entre public et privé

Compte public

- Se comporter comme sur une place publique.
- Vos informations sont disponibles au public.
- Vos paramètres de localisation
- Accès à votre comportement en ligne



La différence entre public et privé



Compte privé

- Permet de masquer des informations.
- Ne permet aucun accès à vos informations sans autorisation.
- Offre plus d'options dans vos paramètres.
- Protège des interactions non désirées



Des bonnes pratiques avec les courriels

Adoptez de bons réflexes

Méfiez-vous des courriels provenant d'inconnus pour :

- Avoir vos informations personnelles ou de l'argent.
- Offrir un prix que vous avez gagné.
- Voir des photos ou des vidéos osés.
- Vous manipuler, vous intimider ou vous offenser.

Portez attention aux :

- Adresses électroniques (expéditeurs)
- Fausses informations ou faux logos
- Liens, boutons ou pièces jointes suspectes
- Fautes d'orthographe
- Langues de communication



Adoptez de bons réflexes



- **Munissez-vous d'un bon anti-virus!**
- **N'ouvrez pas une pièce jointe provenant d'un courriel suspect.**
- **Ne cliquez pas sur un lien ou un bouton suspect.**
- **N'oubliez pas de vérifier le nom de l'expéditeur et l'URL avant de cliquer sur un lien ou bouton.**

Choisir son fournisseur de courriel



Fournisseurs de courriel populaires

Choisir son fournisseur de courriel



Fournisseurs de courriel sécurés

L'avantage de ces alternatives

- E-mails gratuits
- E-mails chiffrés sans publicité
- Données toujours chiffrées
- Aucune adresse IP n'est enregistrée
- Calendrier chiffré et gratuit



Différents courriels - différents comptes

**Les réseaux
sociaux**

Compte1@gmail.com

Messages privés

Compte3@protonmail.com

Divers sites

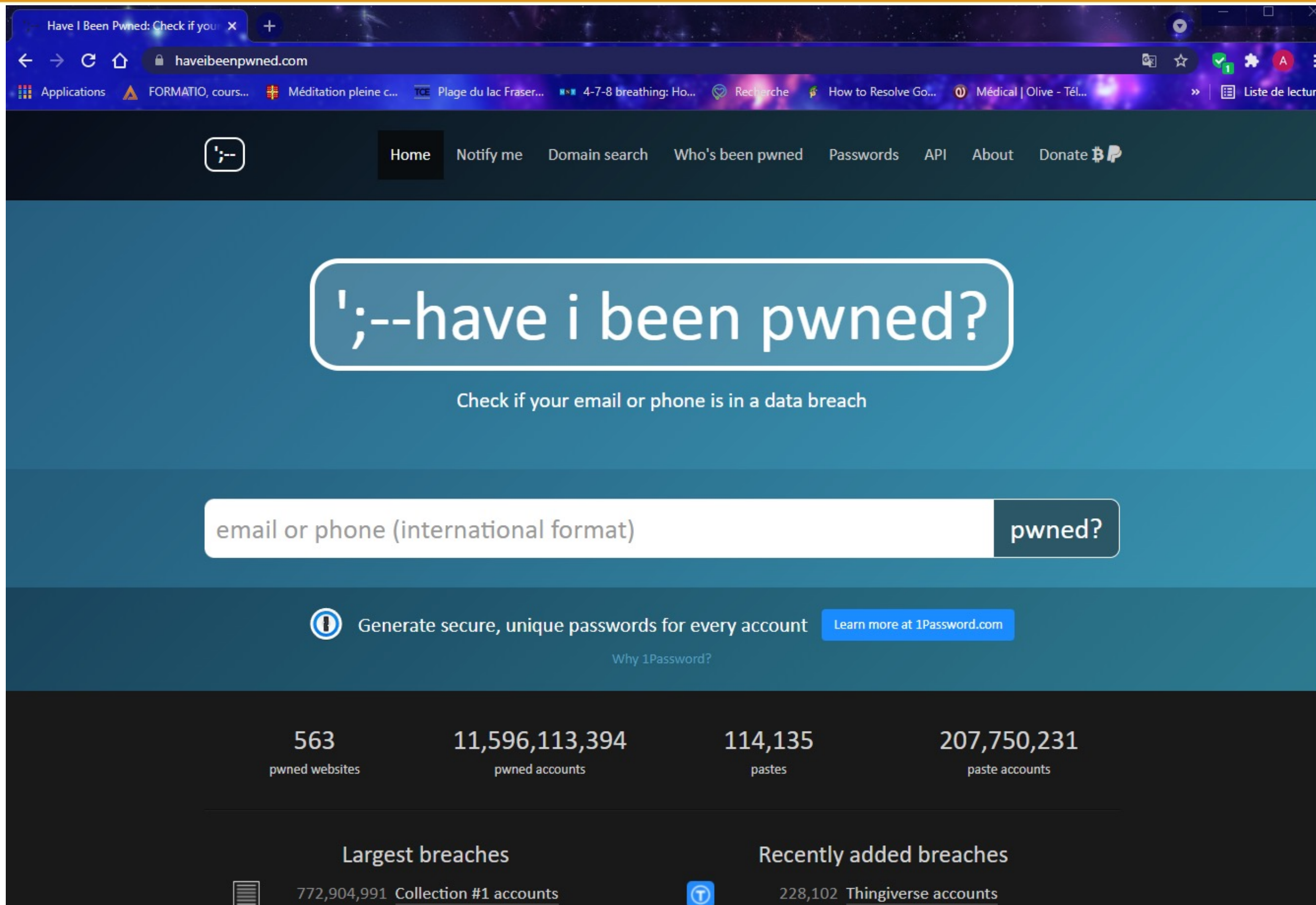
Compte2@hotmail.com

**Pour vos
transactions**

Compte4@hotmail.ca



L'outil haveibeenpwned.com



The screenshot shows the homepage of haveibeenpwned.com. The browser's address bar displays the URL. The website has a dark blue header with navigation links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area features a large input field with the placeholder text "email or phone (international format)" and a "pwned?" button. Below this, there is a section for generating secure passwords, with a link to "Learn more at 1Password.com". At the bottom, statistics are displayed: 563 pwned websites, 11,596,113,394 pwned accounts, 114,135 pastes, and 207,750,231 paste accounts. The footer includes sections for "Largest breaches" (Collection #1 accounts) and "Recently added breaches" (Thingiverse accounts).

Have I Been Pwned: Check if your email or phone is in a data breach

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) pwned?

Generate secure, unique passwords for every account Learn more at 1Password.com

Why 1Password?

563 pwned websites 11,596,113,394 pwned accounts 114,135 pastes 207,750,231 paste accounts

Largest breaches Recently added breaches

772,904,991 Collection #1 accounts 228,102 Thingiverse accounts

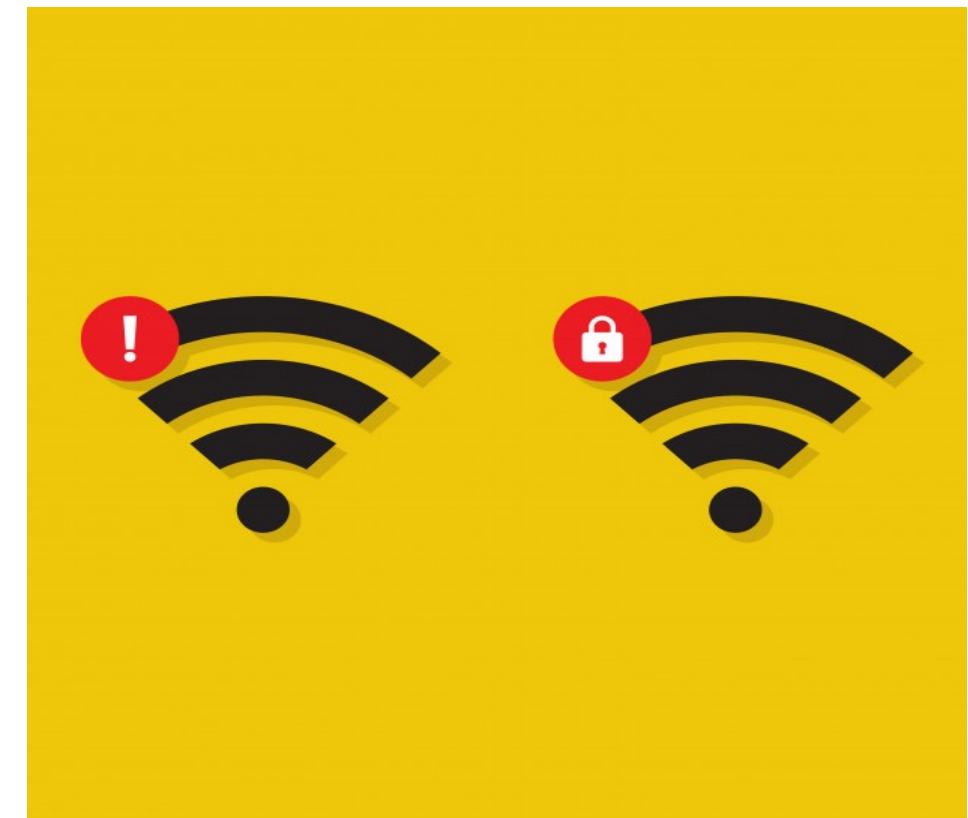
L'importance d'une connexion Internet sécurisée

Risques d'un réseau Internet non sécurisé



Il peut permettre:

- D'accéder à vos informations personnelles.
- D'accéder à divers appareils intelligents.
- D'accéder à vos fichiers, mots de passe etc.
- D'utiliser votre bande passante pour des activités illégales.



Qu'est-ce qu'un VPN ?

Un VPN (Virtual Private Network) est un des meilleurs outils pour protéger votre confidentialité sur Internet.



Les avantages d'un VPN



- Chiffre votre connexion.
- Permet de garder l'anonymat en ligne.
- Est disponible sur divers appareils.
- Permet d'accéder aux sites bloqués.
- Permet de profiter du streaming où que vous soyez.
- Permet d'éviter la censure.
- Ne laisse personne vous pister.

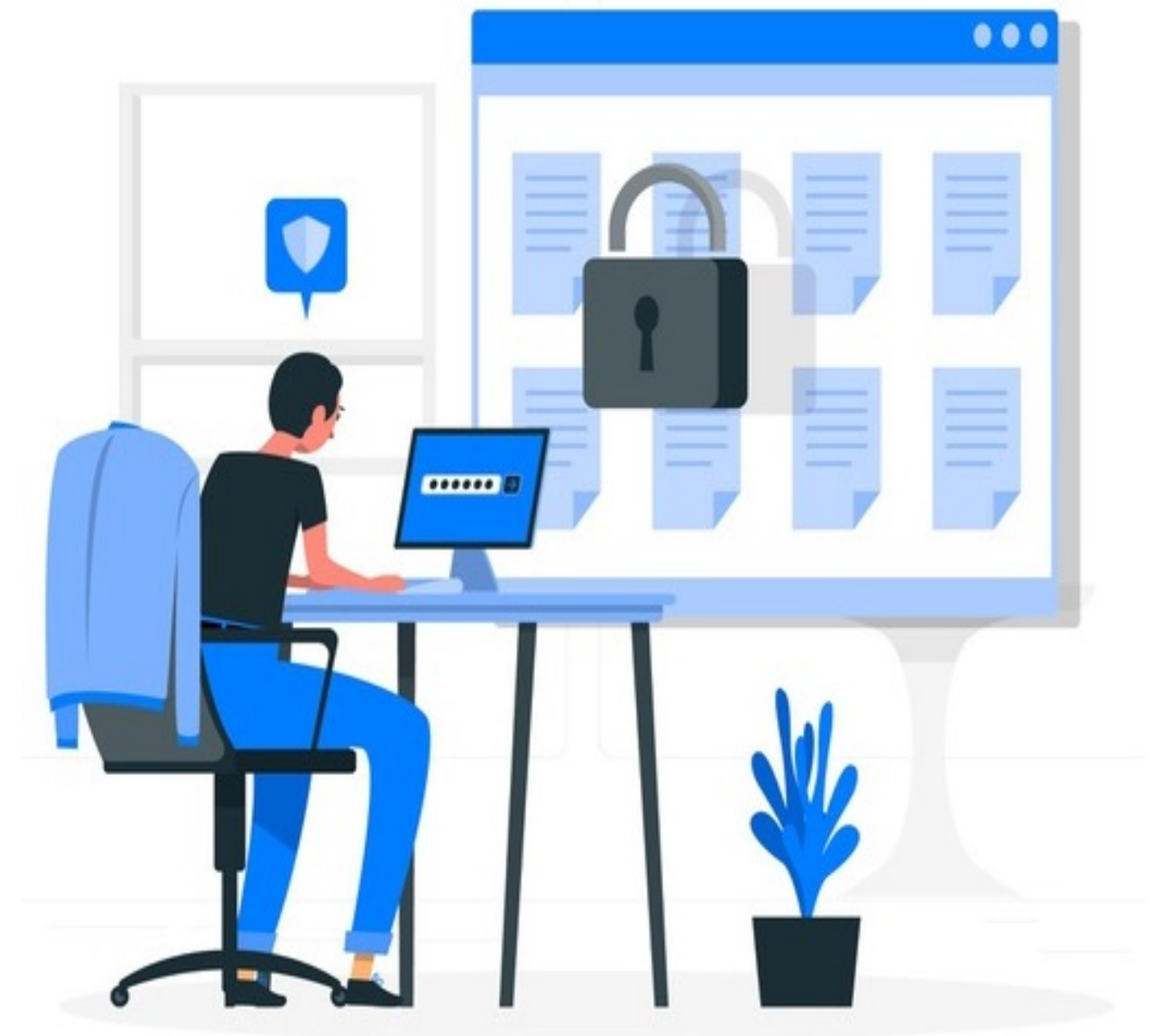




Comment protéger
votre ordinateur et
autres appareils
intelligents

Verrouiller son appareil

- L'option de verrouiller est disponible peu importe l'appareil.
- Elle se retrouve dans les paramètres.
- Elle protège votre appareil des utilisateurs non-autorisés.



Sauvegardez vos fichiers



LES CANADIENS SONT PRÉOCCUPÉS PAR LA SÉCURITÉ **DE LEURS DONNÉES**

43%

sont préoccupés par la possibilité que
leurs données personnelles soient
effacées, altérées ou perdues

35%

sont préoccupés par la possibilité
que leurs données personnelles
soient volées et fassent l'objet
d'une demande de rançon

Sauvegardez vos fichiers



font une sauvegarde seulement
une ou deux fois par année



font une sauvegarde tous
les deux ou trois mois



ne font jamais
de sauvegarde

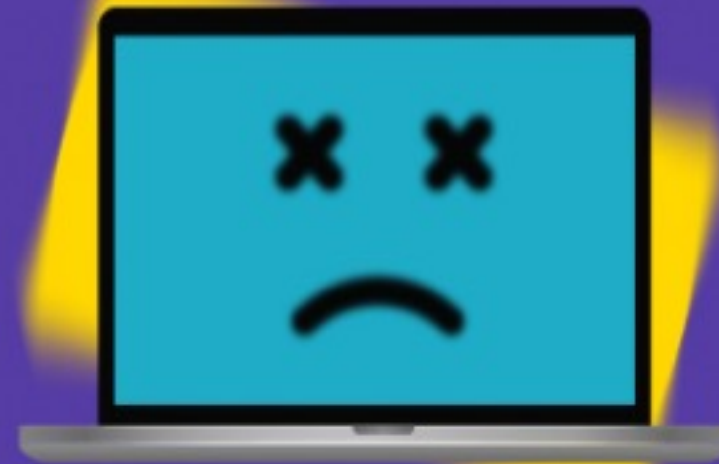
Sauvegardez vos fichiers



VOTRE APPAREIL
FONCTIONNE MAL
OU EST EN PANNE



VOUS ÊTES LA CIBLE
D'UN MALICIEUX OU
D'UN RANÇONGIER



VOUS ÊTES VICTIME
D'UNE PANNE
DE SYSTÈME



VOTRE APPAREIL EST PIRATÉ
OU EST VICTIME D'UNE
ATTAQUE PAR DÉNI DE SERVICE

Sauvegardez vos fichiers



DISQUE DUR EXTERNE

- ➡ peut contenir des fichiers lourds comme des vidéos et des logiciels
- ➡ parfait pour sauvegarder tout le contenu d'un appareil



CD, DVD OU CLÉ USB

- ➡ pratiques, car ils sont facilement transportables
- ➡ conviennent pour sauvegarder des fichiers précis plutôt que tout le contenu d'un appareil



SUPPORT VIRTUEL OU NUAGE

- ➡ peuvent être accédés à partir de l'appareil
- ➡ sont accessibles de partout et en tout temps

Sauvegardez vos fichiers



**SAUVEGARDEZ VOS
DONNÉES AU MOINS
UNE FOIS PAR SEMAINE**



**ACTIVEZ LA SAUVEGARDE
AUTOMATIQUE DE
VOS APPAREILS**



**SAUVEGARDEZ VOS DONNÉES
SUR PLUS D'UN DISPOSITIF
DE STOCKAGE**



L'importance des mises à jour



FAITES RÉGULIÈREMENT LA MISE À JOUR :



du SE de votre
PC et de vos
appareils mobiles



de votre logiciel
antivirus



de votre
navigateur Web



de vos
applications et jeux

L'importance des mises à jour



AFIN DE



profiter de
nouvelles
fonctionnalités

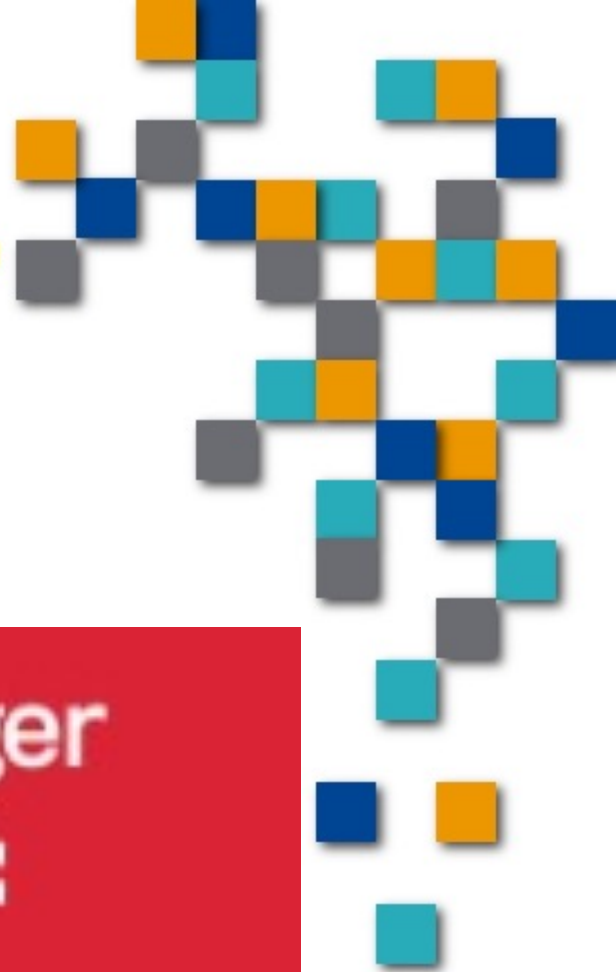


prévenir les
cybermenaces



régler les pépins
et les bogues

L'importance des mises à jour



La façon la plus simple de faire des mises à jour pour protéger vos appareils est de **suivre la règle la plus importante :**

 **ACTIVEZ**  **LES MISES À JOUR** 
 **AUTOMATIQUES** 

Qu'est-ce qu'un antivirus?

Un antivirus permet :

- De naviguer sur Internet en sécurité.
- De détecter des virus.
- De bloquer des accès à des connexions suspectes.
- De supprimer des virus et maliciels.



Choisir un antivirus gratuit ou payant



VERSION gratuite

- Facile à utiliser
- Permet d'essayer plusieurs antivirus
- Fonctions limités
- N'offre pas d'accès à d'autres logiciels

VERSION payante

- Mise à jour régulière
- Offre des produits supplémentaires (anti-maliciel, navigateur privé, etc...)
- Fonctionne avec divers appareils
- Offre de multiples options



Créer des mots de
passe sécurisés

Qu'est-ce qu'un mot de passe?

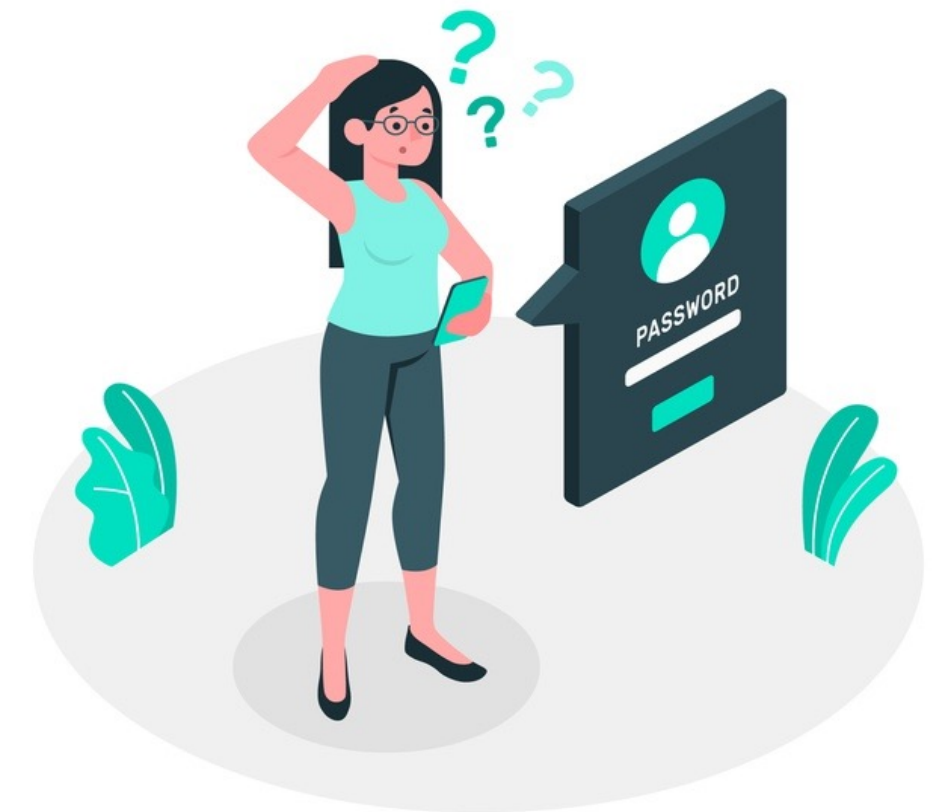
- Un mot de passe permet de sécuriser vos comptes en ligne, l'accès à votre ordinateur ou des documents protégés.
- Vos mots de passe sont personnels et confidentiels.

**Ne divulguez jamais
vos mots de passe.**



Conseils de sécurité pour votre mot de passe

- Personne ne doit connaître votre mot de passe;
- N'utilisez pas le même mot de passe pour plusieurs compte;
- Il doit être long et ne doit pas être facile à deviner;
- Il doit comprendre des lettres majuscules et minuscules, des chiffres et des caractères spéciaux;
- Il ne doit pas inclure votre nom (ou animal de compagnie) ou votre date d'anniversaire;
- Il doit contenir un minimum de 12 caractères.



Conseil pour choisir son mot de passe



1. Choisir 2 à 3 mots au hasard.

formatio **Montréal**

2. Mettre une lettre en majuscule.

formatio **M**ontréal

3. Ajouter des chiffres après chaque mot.

formatio20 **M**ontréal21

4. Séparer les mots avec un caractère spécial.

formatio20! **M**ontréal21

Une phrase de passe plutôt qu'un mot de passe



1. Trouver une phrase facile à retenir.

J'ai un chat blanc et un chien noir.

2. Garder la première lettre de chaque mot et les chiffres.

Ja1cbeucn

3. Ajouter des caractères spéciaux.

Ja1?cbeucn!

Gestionnaire de mot de passe

- Une base de données de vos mots de passe.
- Un seul mot de passe à retenir.
- Génère des mots de passe longs et complexes



Gestionnaire de mot de passe



Différent gestionnaire de mot de passe :



1Password



KeePass

LastPass ****

Gestionnaire de mot de passe

Un bon gestionnaire de mot de passe offre:

- L'authentification multifactorielle
- Une invitation à modifier les vieux mots de passe
- La notification des mots de passe faibles ou déjà utilisés
- L'intégration à vos autres appareils



Gestionnaire de mot de passe



**Trousseau
(keychain) Icloud**

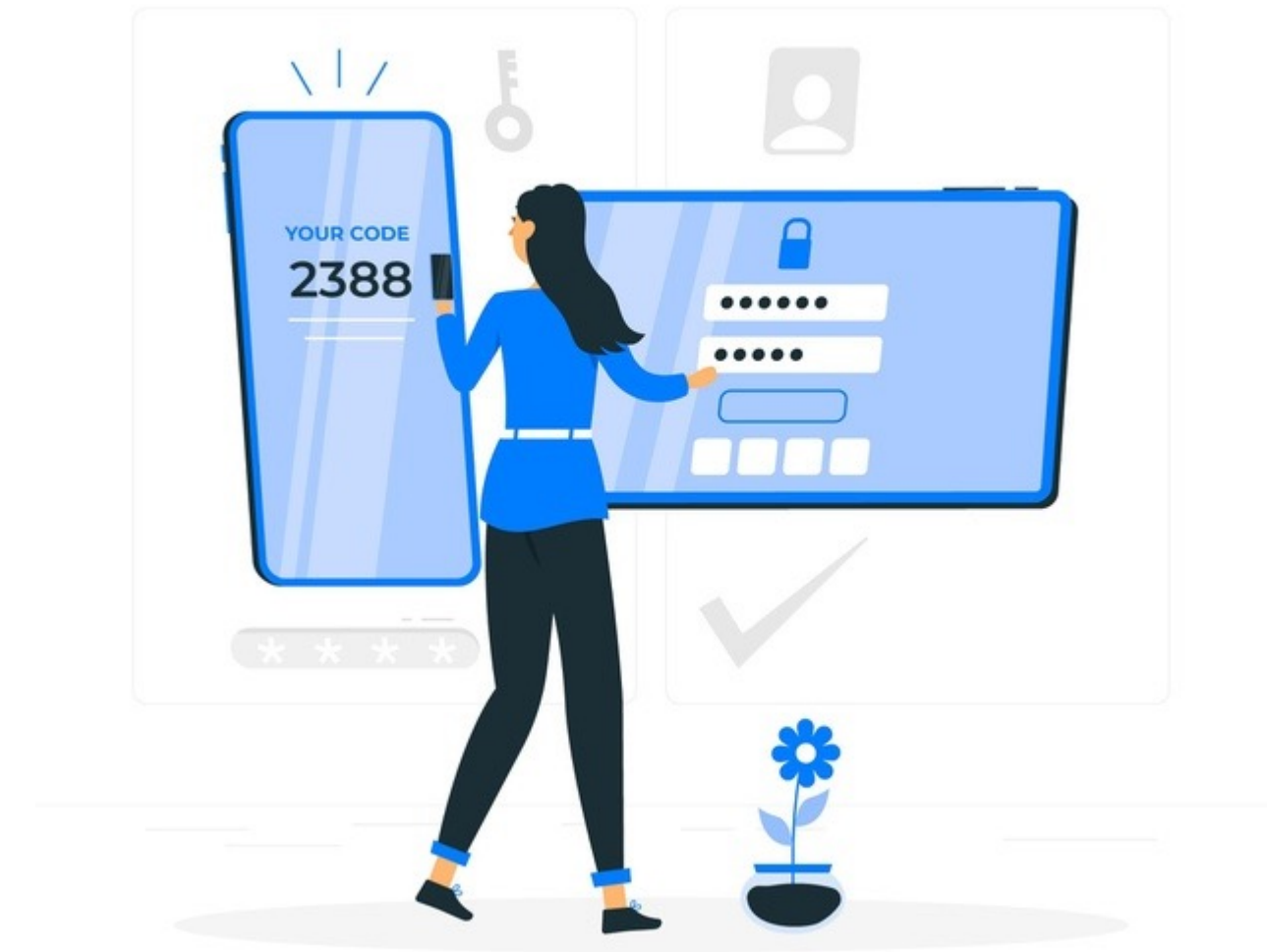


**Gestionnaire de mots
de passe Google**

Authentification multifactorielle

Plusieurs termes:

- Double authentification,
- Connexion en deux étapes,
- 2-Step Vérification,
- Authentification forte.



Authentification multifactorielle

Demanderà une information à partir de:

- Ce que vous savez : un NIP, un mot de passe ou une question de sécurité
- Ce que vous possédez : votre téléphone
- Ce que vous êtes : vos empreintes digitales, votre visage, vos yeux ou votre voix



Authentification multifactorielle



Activez l'authentification multifactorielle chaque fois que cela est possible.

Questions typiques de sécurité

- Quel est le nom de votre animal de compagnie?
- Quel est le nom de jeune fille de votre mère?
- Quel est le nom de votre chanson préférée?
- Quel est votre passe-temps favoris?
- Quelle est votre ville préférée?
- Quelle est la marque de votre première voiture?
- Quel est l'endroit où vous êtes né(e)?
- Quelle est votre équipe favorite?

Attention à
votre réponse





Questions Quiz

Mise en situation



Vous recevez un appel vous demandant vos données personnelles et financières pour que le crédit d'impôt relatif à la taxe sur le carbone de l'Ontario soit déposé dans votre compte. On vous demande également d'adhérer à des services de garantie et de protection résidentielle.

Est-ce une fraude?

Alerte à la fraude!



Signes

- Appels offrant des avantages fiscaux du gouvernement.
- Appels non sollicités vous demandant des renseignements personnels ou bancaires.
- Appels non sollicités vous demandant de confirmer des données personnelles et financières.

Protégez-vous!

- Apprenez-en plus sur les crédits d'impôt offerts par le gouvernement fédéral et les provinces.
- L'accès aux services gouvernementaux est gratuit.

Mise en situation



CALL TOLL FREE +1-844-483-8886

Est-ce une fraude?

Alerte à la fraude!



Signes

- Appels à installer un logiciel d'accès à distance.
- Communication au moyen de fenêtres publicitaires sur des sites Web dans lesquels on vous demande d'appeler le numéro à l'écran immédiatement.
- Messages ou appels non sollicités vous demandant des renseignements personnels.
- Appels non sollicités vous demandant de confirmer des données personnelles et financières.

Protégez-vous!

- Apprenez-en plus sur les fraudes de soutien technique.
- Ne cliquez aucun lien et fermez la fenêtre web.
- Ne partagez pas des informations personnelles.

Parmi ces réponses, que pourriez-vous proposer un arnaqueur ?

- A) Une grosse somme d'argent
- B) Un prix gagné
- C) Une photo ou vidéo osée
- D) Une relation amoureuse
- E) Toutes ces réponses

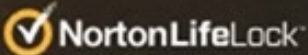


Quels sont les problèmes rapportés par mon antivirus?



f [redacted]

Mon Norton





 PROTÉGER UN AUTRE APPAREIL
1 SUR 5 LICENCE(S) UTILISÉE(S)



Sécurité de l'appareil

Vous êtes vulnérable.

ANALYSE RAPIDE | LIVEUPDATE

Corriger

▼



Secure VPN

Votre connexion n'est pas protégée

Activer

▼



Sauvegarde cloud

Données vulnérables

Corriger



Password Manager

Stockez et renseignez vos mots de passe

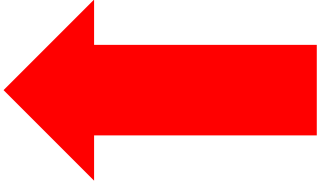
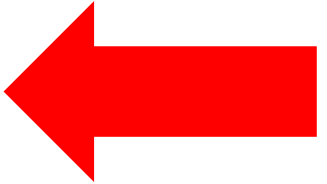
Configurer



Contrôle parental

Protégez vos enfants en ligne

Gérer



FORMATIO

RESSOURCE
INFORMATIQUE
BUREAUTIQUE



Six commandements de Stormshield

Six commandements de Stormshield



1- À nettoyer, tu te mettras à:

- Détruire les cookies et historique de navigation tous les 3 mois.
- Nettoyer les courriels, boîte aux lettres, corbeille, envoyés.
- Enlever les applications inutilisées ou installées pour “essayer”.
- Nettoyer le disque dur.

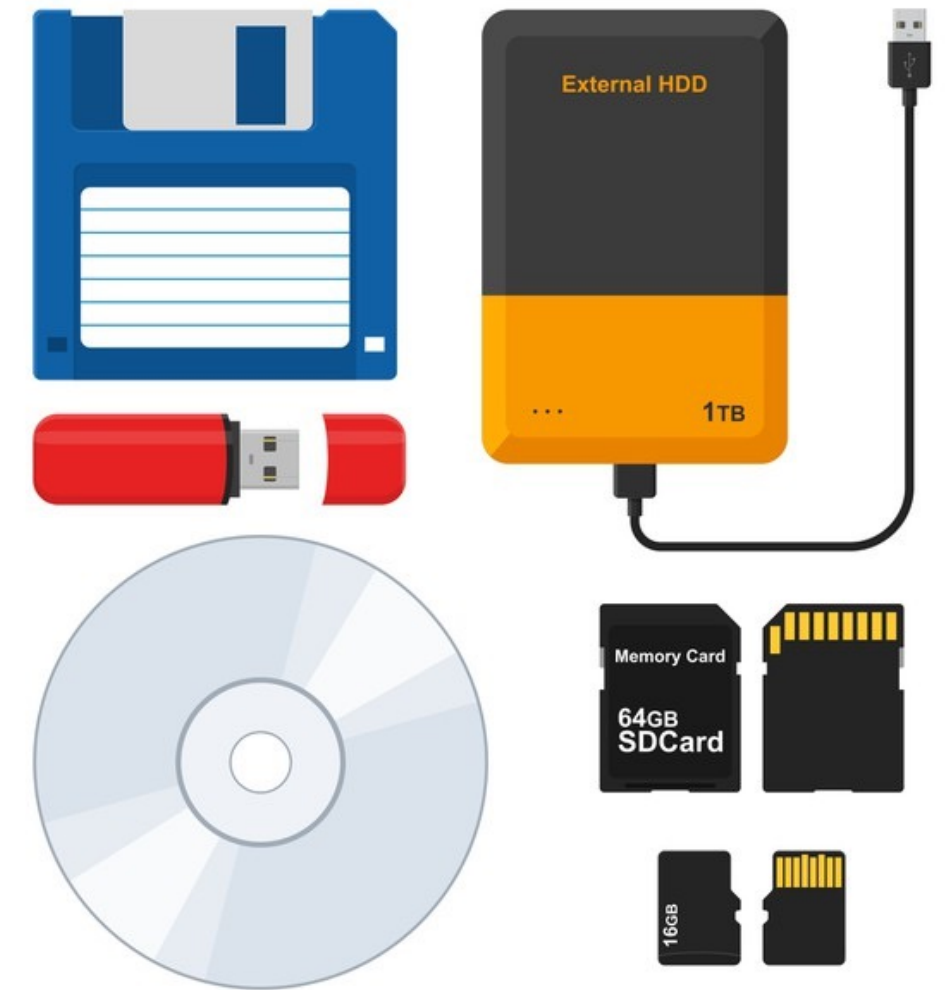


Six commandements de Stormshield



2- Automatiquement, tu sauvegarderas:

- Copie des fichiers sur un deuxième disque, sur une clé USB ou sur le cloud externe ou personnel.



Six commandements de Stormshield



3- Pour se protéger, il faudra:

- Utiliser un antivirus et des détecteurs de maliciels.
- Utiliser l'identification à deux facteurs.
- Favoriser les sites https (cryptés).
- Se brancher à des réseaux sécurisés.
- Utiliser un VPN.



Six commandements de Stormshield

4- Dans un courriel douteux, tu ne cliqueras point.

Il faut:

- Détecter les courriels douteux.
- Vérifier l'adresse de l'envoyeur.
- Éviter de se connecter à ses sites bancaires (ou importants) via le courriel frauduleux.

Les pourriels sont la principale source de spam, phishing, etc...



Six commandements de Stormshield



5- Mots de passe, tu écriras en:

- Utilisant des phrases de passe,
- Utilisant des logiciels spécialisés,
- Formant des mots de passe complexes, fréquemment modifiés, jamais divulgués.



Six commandements de Stormshield



6- Ton argent doublement, tu protégeras.

- Toutes données n'ont pas la même valeur
- Prudence avec vos finances et sites connexes
- Cartes de crédits sous contrôle



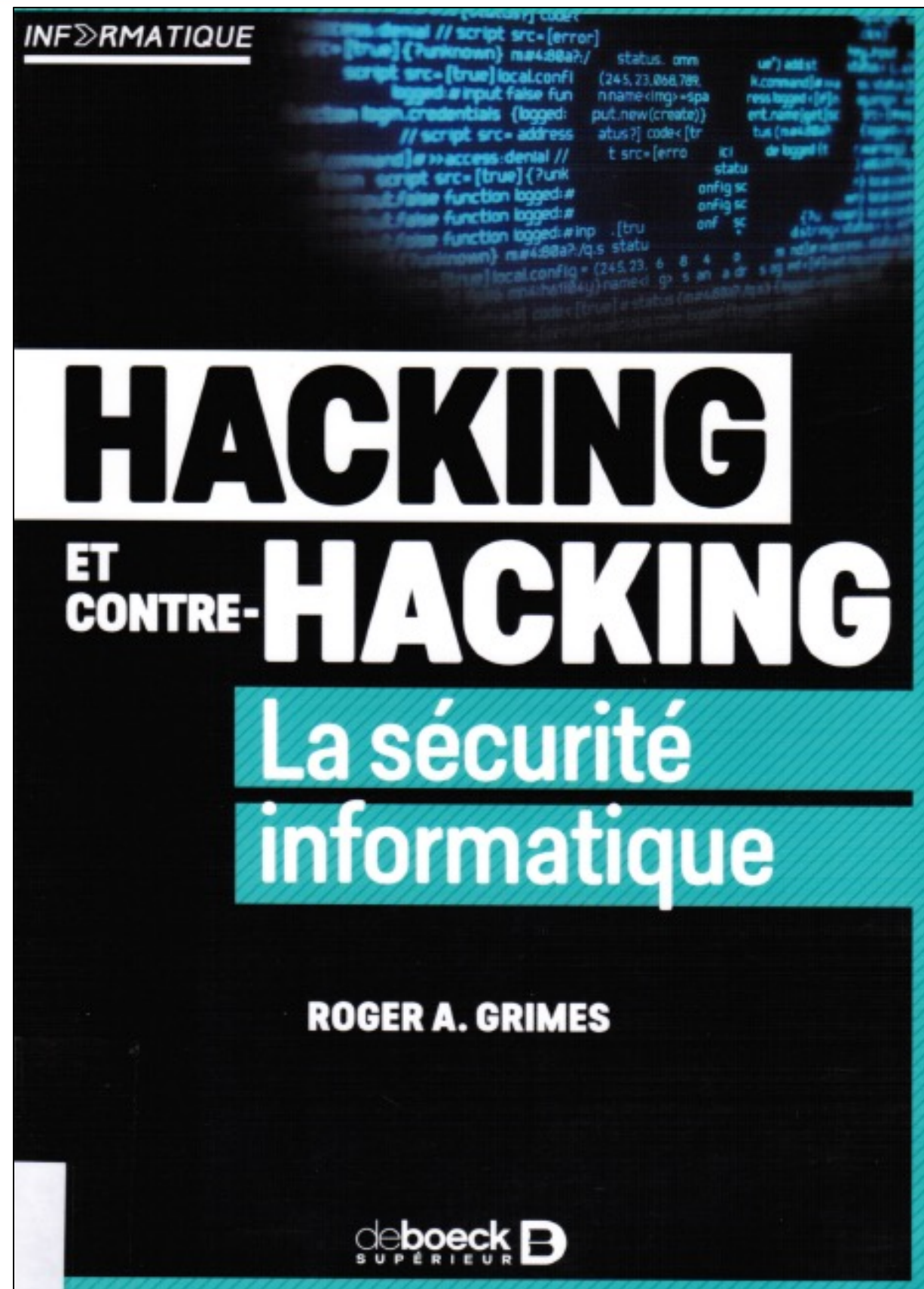
Commandement de FORMATIO



Tu ne divulgueras pas tes données personnelles : adresse, âge, sexe, etc...



Vous face à la sécurité



Les problèmes les plus compliqués de sécurité informatique ne concernent pas la technologie, **mais bien la manière dont nous utilisons la technologie** en combinaison avec toute la sociologie, la politique et l'économie que la sécurité informatique implique.
Extrait P45



«L'hygiène numérique» peu enseignée



Dominique Scali | Journal de Montréal
| Publié le 18 mars 2019 à 21:29 - Mis à jour le 18 mars 2019 à 21:37

Adoptez les bons réflexes



En général:

- Ne cédez pas à la pression, à l'urgence de la demande.
- Ne cliquez sur aucun lien si le message est douteux ou si vous ne connaissez pas l'expéditeur.
- Ne donnez aucune information personnelle, surtout si vous ne connaissez pas le destinataire.
- Vérifier si le site est bien sécurisé et utiliser le site web de l'institution.
- Informez-vous auprès de vos amis, famille et organismes indépendants.
- Utiliser des mots de passe complexes ou des phrases de passe.
- Signaler une fraude à la Police ainsi qu'au centre Antifraude du Canada.

N'oubliez pas que...

**La prudence
est toujours votre
meilleure protection!**



Coordonnées de FORMATIO



www.formatio.info



[Facebook.com/formatio.info](https://facebook.com/formatio.info)



(450) 656-3348



info@formatio.info