

Bienvenue au webinaire



« Reprendre sa souveraineté numérique »

Testing, one-two!

- M'entendez-vous bien?
- Voyez-vous le clavardage? Les questions c'est par-là. Les compliments aussi.
- Attache ta tuque, ca dure 1h30 non-stop!
- Questions-réponses 30 minutes à la fin.

On va parler de kôa?

- De comment on s'fait fourrer depuis si longtemps, par Big Tech;
- De pourquoi la vie privée sur le web c'est mega important;
- De comment affaiblir ces grosses compagnies par divers gestes, certains simples, certains complexes;
- De changer le monde, ni plus ni moins.



C'est qui ce gringo qui parle?



Moi c'est Alex!

- Dirigeant d'une agence web depuis 2014
- Passionné de santé depuis très jeune
- Étudiant en naturopathie
- Un maudit français qui remet tout en question dans la vie
- Donc un complotiss' bien sûr
- Un gars qui œuvre dans la matrice et dehors en même temps
- Un mangeur d'ordinateur depuis l'âge de 11 ans

Mon intention ♥

- Que vous preniez conscience que votre vie privée est sans cesse en danger, sans que vous le sachiez;
- Que vous repartiez du webinaire avec 1, 2 ou 15 actions que vous pouvez entreprendre, et qui contribueront à changer le monde positivement;
- Que vous transmettiez ces connaissances (et ce webinaire) à tous ceux qui peuvent y être intéressés.

Un webinaire pour tous les niveaux



*Kossé ça un vé-pé-énne?
S'tu le nouveau nom du parti conservateur?*

Pourquoi notre vie privée sur le web importe tant

- Vol d'identité
- Fraude
- Traçage
- Profilage, ciblage
- Manipulation d'opinion et de narratif médiatique
- Réputation sociale
- Envoi d'infos aux autorités gouvernementales
- Étalage d'infos aux employeurs et stalkers
- Censure
- Donner de plus en plus de pouvoir aux GAFAM pendant que les « vrais » meurent de faim



Quelques abominables faits

2013 - Edward Snowden : il est devenu célèbre en 2013 en divulguant des informations classées secrètes sur les programmes de surveillance de masse menés par les agences de renseignement américaines et britanniques, notamment la NSA et le GCHQ. Il a révélé que ces agences surveillaient les communications électroniques à l'échelle mondiale, collectant des données sur des citoyens ordinaires sans leur consentement. Cette révélation a suscité un débat mondial sur la vie privée, la sécurité des données et les limites du pouvoir des agences de renseignement.

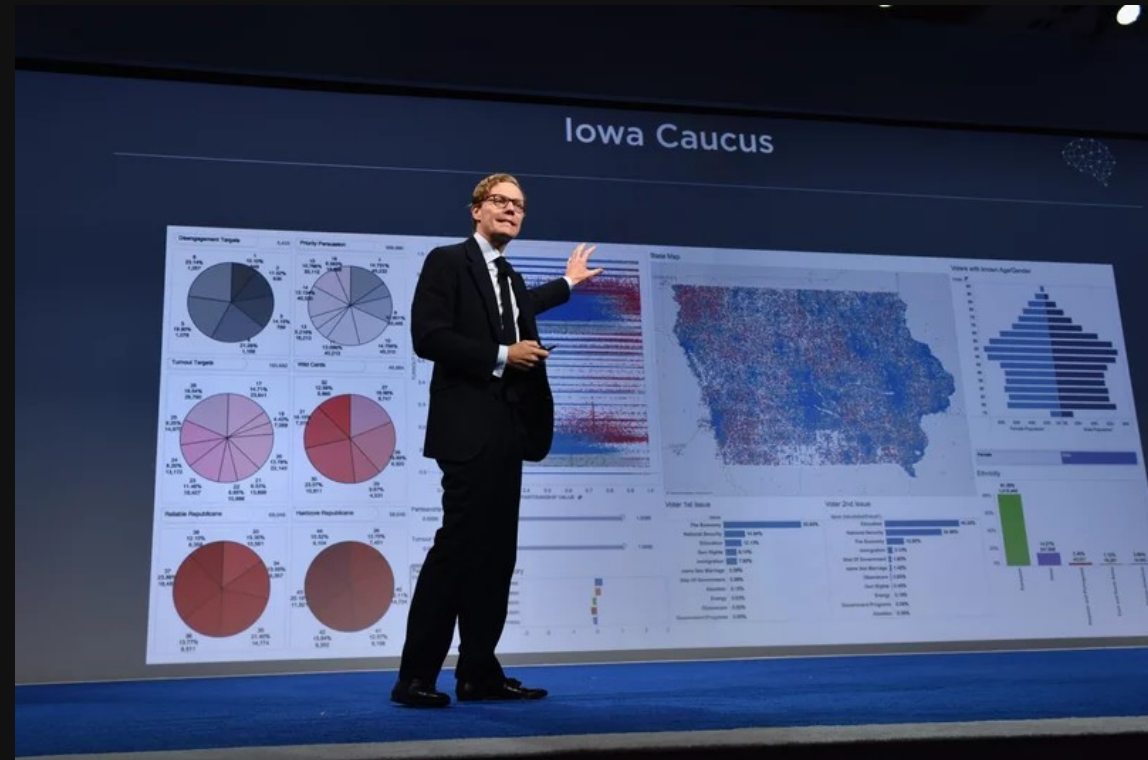


Meta' la prison

- Avril 2021 : un forum de hack affiche des données sensibles de 530 million de comptes Facebook : téléphone, lieux, dates de naissance et plus. 265 euros d'amende.
- Juin 2020 : Facebook partage accidentellement les données de tous ses utilisateurs avec les développeurs Facebook
- Déc 2019 : 309 million de comptes Facebook compris par un groupe de hackers
- Mars 2019 : 600 million de mots de passe Facebook sont stockés en texte clair dans un serveur depuis 2012
- Dec 2018 : découverte que Facebook partage des informations d'utilisateurs sans permission à 150 entreprises dont Netflix et Spotify.

Le scandale 2018

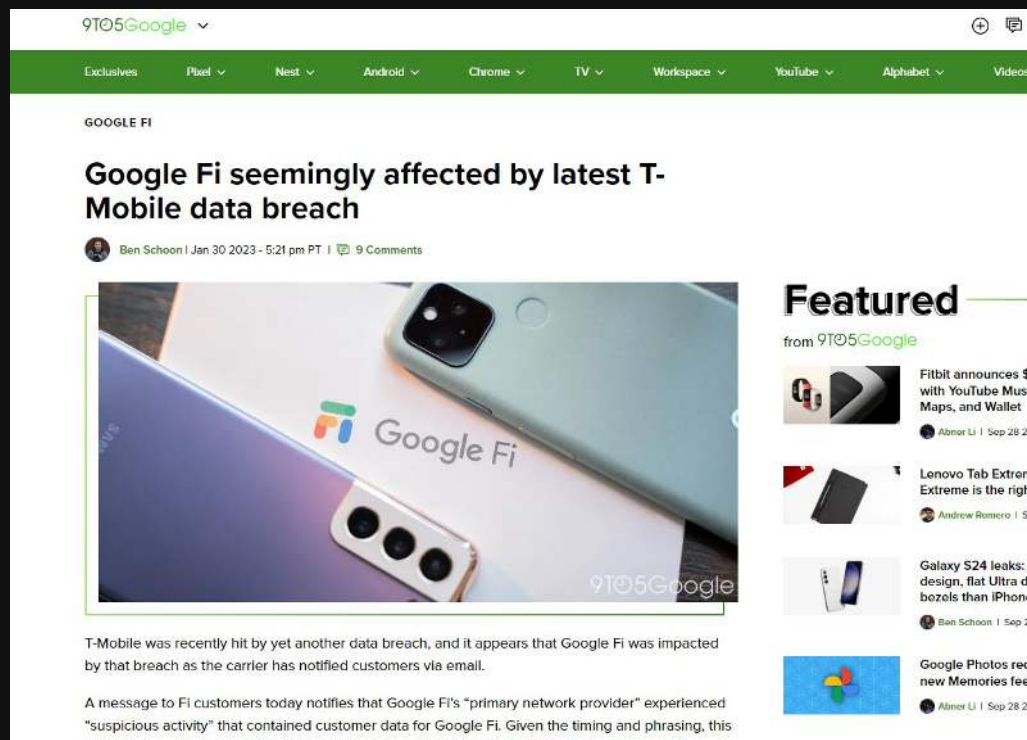
Mars 2018 - scandale du Cambridge Analytica : une faille majeure de Facebook permettant à une firme politique de collecter 87 million de données sur les utilisateurs de la plateforme



<https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election>

Dégoût-gueule

Janvier 2023 : Google Fi se fait hacker. 37 million de clients de l'opérateur T-mobile voient leurs informations fuitées.



<https://9to5google.com/2023/01/30/google-fi-data-breach-tmobile/>

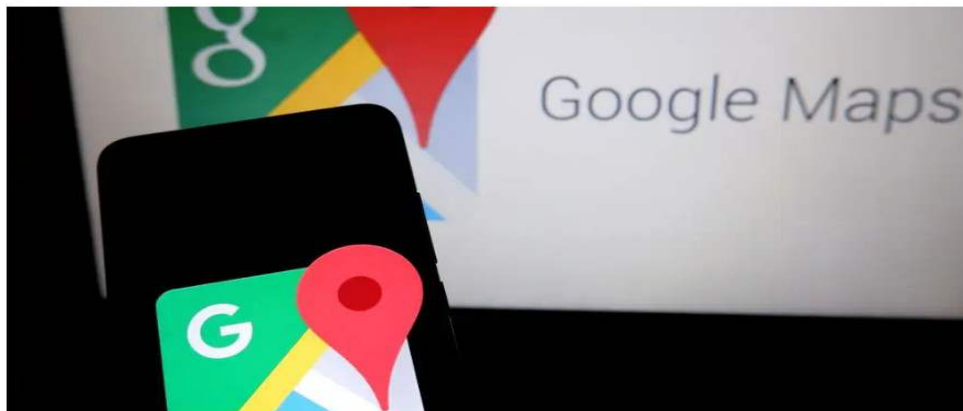
T'es allé où hier soir, à 22h?

2020 : un résident est devenu suspect numéro 1 dans une investigation. La police locale a forcé Google à divulguer ses données de localisation. Les données montraient qu'il prenait fréquemment le vélo à côté de la scène de crime.

HOME > NEWS

A Florida man was made a suspect in a burglary after police used Google location data from a fitness app

Ellen Cranley Mar 7, 2020, 1:56 PM UTC-5



Avishek Das/SOPA Images/LightRocket via Getty Images

- A 30-year-old resident of Gainesville, Florida was made a suspect in a burglary because of location data that was recorded in a fitness app.

Le CV de Google

- Dec 2018 : google + expose les données de 52,5 millions d'utilisateurs
- Mars 2018 même brèche et Google n'informe personne
- Sept 2014 : 5 million de mots de passe Gmail fuités
- 2009 : un groupe de hacker du gouvernement chinois s'infiltrant dans les serveurs de Google, Yahoo et d'autres compagnies US pour vérifier des informations sur des activistes du droit humain chinois
- 2020 : condamnation à 5 milliards pour tracker toutes les activités sur le navigateur Chrome même en incognito
- Sept 2019 : condamnation de 170 million pour collecter des informations relatives aux enfants de – 13 ans sur YouTube for kids
- Août 2018: Google traque les données de localisation à 2 milliards d'utilisateurs sans leur permission
- Et tellement plus de fuites encore...

Amazon(e) dangereuse

- Juillet 2021 : condamné à 746 million \$ pour violer les réglementations en matière de confidentialité (GPDR) sans scrupule ([source](#))
- Oct 2020 : deuxième fois qu'un employé utilise un grand nombre de données clients pour les vendre à des entreprises externes ([source](#))
- Mars 2023, un groupe de hacker s'infiltrèrent dans l'appareil de sécurité d'Amazon Ring. ([source](#))
- Nov 2018 : les courriels et noms de tous les clients sont fuités sur le web, 2 jours avant le black friday ([source](#))
- Sans compter toutes les failles des services Amazon (comme AWS)

Apple, un saint?

- Juillet, août et septembre 2022 : Apple met à disposition 3 patchs pour une faille majeure dans ses téléphones. Apple n'explique rien sur ces failles et leurs conséquences.
- Sept 2021 : un logiciel malveillant israélien appelé « Pegasus » infecte les appareils Apple. Le logiciel pouvait enregistrer les appels, les messages, activer les caméras et micros sans que l'utilisateur ne s'en aperçoive. Le groupe de hacker travaille activement à la création de spywares pour les gouvernements (Mexique, Arabie Saoudite) afin de surveiller les terroristes, criminels, activistes, journalistes et politiciens. ([source](#))
- Janvier 2019 : les chercheurs de Google découvrent une faille sur les iPhones permettant de voler les contacts et mots de passe juste en allant sur un site web malveillant ([source](#))
- En 2014, une fuite immense a lieu sur iCloud, faisant fuiter les photos nues de plusieurs centaines de célébrités et probablement vos photos aussi. Apple nie. En bloc.,

Quelques faits cocasses

- Août 2023 : 760000 utilisateurs sur Discord voient leurs informations fuiter, comme le courriel, adresse et mots de passe cryptés. Le tout était vendu sur un forum pour pas cher en plus.
- Juillet 2023 : l'OTAN se fait hacker son portail pour les communautés d'intérêt pour la coopération. Plusieurs documents non classifiés et données sensibles sur les utilisateurs du portail fuient.
- Même mois, les agences aux US se font hacker par la Chine via Microsoft Cloud
- Juin 2023 : 101000 utilisateurs hackés sur ChatGPT. Leur ID et mots de passe sont fuités, et certains se font contaminer par un logiciel malveillant.

Bon ben, je déclare forfait!



- « Ils sont trop big, on n'est rien pour eux »
- « C'est trop tard! Ça fait des années que je nourris Big Tech »
- « Ouf ça va être trop difficile de mettre en place des changements »
- « Je n'ai pas le temps et l'énergie de faire quoique ce soit pour changer mes habitudes »

Naviguer sur internet



Navigateurs

- Brave 
- Firefox : Focus (Android/iOS), Librewolf (Windows, macOS) 
- Vanadium (GrapheneOS) 
- Tor 

Tests de navigateurs : privacytests.org

Penser à configurer le blocage du tracage sur les sites  :
anti-tracker, anti-publicité, empreinte numérique, cookies
interdomaine

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

Moteurs de recherche

-  Qwant
-  Brave Search (mais attention, entraînement de IA : source)
-  Presearch

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

VPN

-  Proton VPN
-  iVPN
-  Mullvad VPN
-  Wireguard
-  Above VPN (d'Above suite) et Wireguard

Conseils :

-  Éviter de se connecter à un Wi-Fi sans VPN, surtout dans une zone publique.
-  Éviter les sites sans certificat SSL (https://)
-  Activer killswitch sur VPN

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

Limiter son exposition

-  Limiter les comptes créés sur le web
-  Supprimer les comptes inactifs autant que possible
- Créer ses comptes avec de fausses informations :
 -  Alias pour le courriel (simplelogin)
 -  Jamais la date de naissance
 -  Questions de sécurité aléatoires
-  Désinscrivez-vous aux infolettres (Cleanfox)

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

Courriels

-  ProtonMail (suite incluant gestionnaire de mots de passe, cloud, calendrier, VPN) – attention fuite de données aux autorités (source)
-  Courriels sur serveur privé (Collectif HUB)
-  Courriels sur la suite Above Suite

-  Utiliser des alias autant que possible
-  Faire attention au spam et au phishing (hameçonnage)

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

Téléphone mobile



Passer au téléphone stupide

IOS / Android, la même bouette!

-  Repasser aux téléphones stupides (Nokia, BlackBerry , ligne résidentielle avec fil, etc...)
-  Above Phone avec GrapheneOS
(rabais de 25\$ avec le code ABOVEAIDE)

Couvrez votre caméra (Wikihow)

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

Les apps'

La majorité des applications sont des logiciels malveillants.

- Utiliser une alternative opensource
- ✓ Utiliser la version du navigateur
- ✓ Supprimer les applications inutilisées ou secondaires

Des alternatives open-source :

K9 Mail pour le courriel, New Pipe for Youtube, VLC ou Vinyl pour la vidéo, Exodus pour les wallets, Librera FD pour la lecture de documents, Magic Earth et OSM pour le GPS

Codification :

✓ Facile à appliquer | ● Nécessite quelques efforts | ● Aisance informatique requise

Communication

- ✓ Les textos et appels sont surveillés! Éviter.
- Utiliser des applications en ligne telles :
 - Telegram FOSS
 - ✓ Signal
 - XMPP
- Privilégier le no-SIM (Above Phone, ChatR?)

Codification :

✓ Facile à appliquer | ● Nécessite quelques efforts | ● Aisance informatique requise

Le nuage (cloud)



Des chemtrails dans le cloud

É-VI-TER les cloud à tout prix, et soyez méfiants de ceux qui ont l'air de confiance.

Serveur en US = espionnage par le gouvernement

-  Utiliser le bon vieux CD ou disque dur externe pour sauvegarder ses données
-  Utiliser un serveur privé canadien ou au Pays Bas pour stocker ses données
 - Dediseedbox (inclut une suite d'outils, dont Plex)
-  Supprimer vos photos des cloud type iCloud, Google Photos et compagnie
-  Vendez vos caméras et moniteurs pour bébé

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

Sécurité sur ordinateur



Système d'exploitation

Microsoft et Apple : même bouette encore!

- ● Adopter Linux
- ● Sauter sur les nouveaux futurs ordinateurs Above
- ● Utiliser Windows et supprimer le maximum d'applications fournies par votre ordinateur
- ● Faites-vous monter votre ordinateur sur mesure

Codification :

✓ Facile à appliquer | ● Nécessite quelques efforts | ● Aisance informatique requise

Sécurité

-  Ajouter un antivirus (Bitdefender)
-  Scan d'outils malveillants (MalwareBytes)
- Utiliser un logiciel de gestion de mots de passe
 -  Keepass (local)
 -  Keeper Security (cloud)
-  Activer la double-authentification sur tous vos comptes
-  Éviter tout bonnement les sites dangereux ou suspects
-  Privilégier la connexion au câble que celle au Wi-Fi
-  Privilégier les logiciels opensource (VLC, Libreoffice, GIMP...)

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

A person wearing a red hoodie and a Guy Fawkes mask is shown in the center of the frame, holding two smoke bombs. One bomb is being thrown to the left, creating a large plume of white smoke. The other is being thrown to the right, creating a large plume of dark smoke. The background is a blurred urban setting with brick walls and a window.

**D'autres
aspects à
considérer**

Médias sociaux

- ● DE-TOX! Ça vous fera du bien!
On essaie de réduire tranquillement chaque semaine, puis on suspend son compte.
On s'observe durant.

ALTERNATIVEMENT :

- ● s'inscrire sur son réseau social incognito
- ✓ interagir le moins possible
- ✓ exposer le moins possible de données sensibles et supprimer celles existantes



Codification :

✓ Facile à appliquer | ● Nécessite quelques efforts | ● Aisance informatique requise

Vidéo conférence

-  Jitsi
-  Signal
-  Telegram
-  XMPP
-  Utiliser la version web de Zoom et Teams
-  Éviter toute installation de logiciel de vidéoconférence

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

Appareil « intelligent »

-  On dégage de la maison tous les appareils intelligents : ampoule, frigo, voiture, Alexa, Chromecast, caméras en ligne, aspirateur, etc.
-  On opte pour des produits totalement déconnectés du web

Codification :

 Facile à appliquer |  Nécessite quelques efforts |  Aisance informatique requise

Monnaie numérique

- ● Points JEU
- ✓ Cash au lieu de carte
- ● Troc
- ● Cryptomonnaies : Monero, BTC
- ● Wallets sans KYC (anonyme) comme Exodus



Codification :

✓ Facile à appliquer | ● Nécessite quelques efforts | ● Aisance informatique requise

Pis t'en as eu assez?

Pour offrir une contribution :

- Interac à info@le-caribou.ca
réponse : souverain
- Bitcoin (BTC) :
bc1q9auvw8xxjakqcyc3jnjupx3vkpxupqu
dj5skhe
- Monero (XMR) :
43BCR1gUP5SYKHWTTX2m6a882Ppfgwts
MZbYYXiThxfdNHZfoBWePJEUXHpqfUQW
ZFFWxqofeeYJZTKCbUPzom4aCTpbpaZ



Codification :

✓ Facile à appliquer | ● Nécessite quelques efforts | ● Aisance informatique requise



**Questions?
J'ai sûrement la
réponse!**