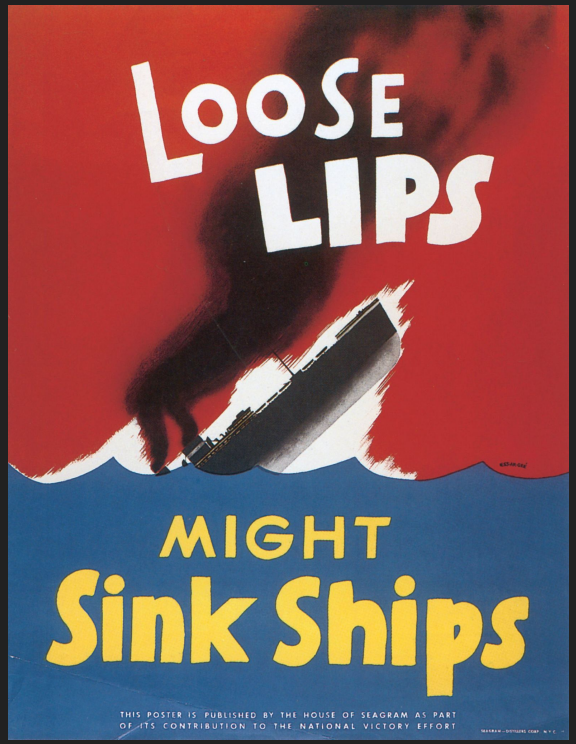
OpSec et vie privée 101

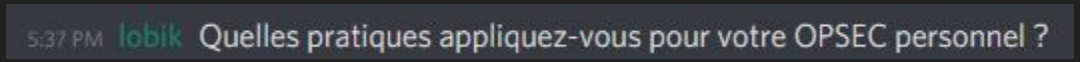
VN
&
Riga

QuebecSec 2021



Idée

- Sujet évolue vite, beaucoup d’infos et parfois spéculations...
- Répondre à une question par du concret
- Sensation d’être pris en otage
- Pas beaucoup d’éducation sur le sujet



Nous

- VN : Analyste en sécurité, membre comité HF, Rocket League, BBQ
- Riga : Analyste en sécurité, OSINT aficionado, pentester

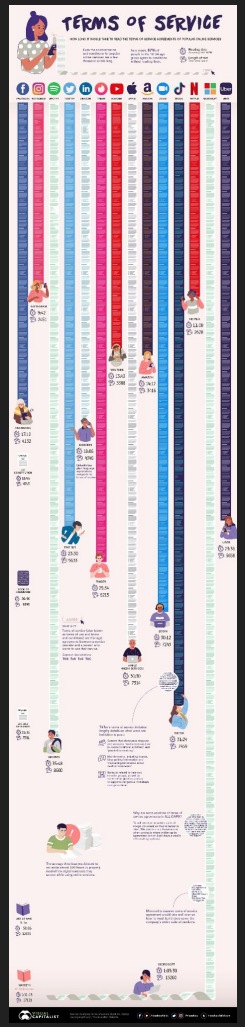
Disclaimer : le contenu de cette conférence n’engage que nous et aucunement nos employeurs

À se souvenir

- Paranoïa vs information factuelle - relatif au modèle de risque
- **Jamais** un point de vue définitif, il est encouragé de faire ses propres recherches et s'informer régulièrement
  - Challengez-nous!
- Nous voulons surtout démarrer la discussion et la curiosité sur le sujet
- On ne parlera PAS de :
  - Comment Facebook, Tiktok et autres sont mauvais - contrats d'utilisation
  - Pratiques insouciantes (ex: parents de toute l'école en Cc et accès édition au formulaire)
  - Surveiller ce qu'on poste en ligne
    - Ex: quand on part en vacances, ce qui peut être utilisé contre nous
  - Arnaques communes
- Cette présentation est une introduction, un début de piste.

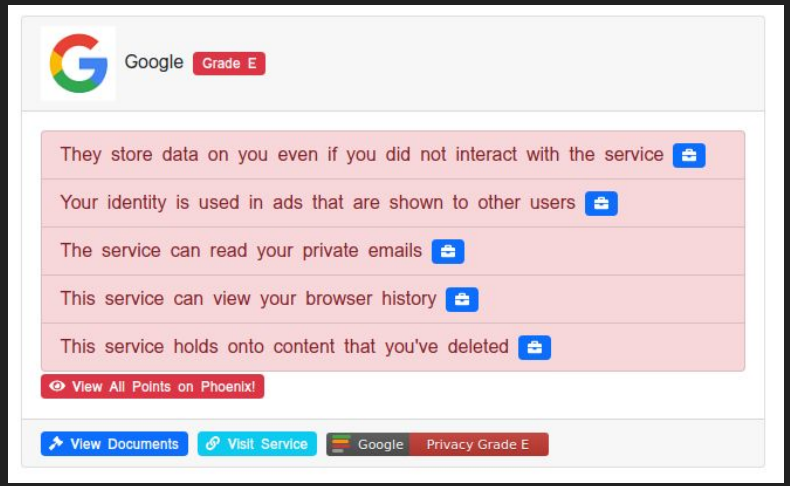
Services en ligne

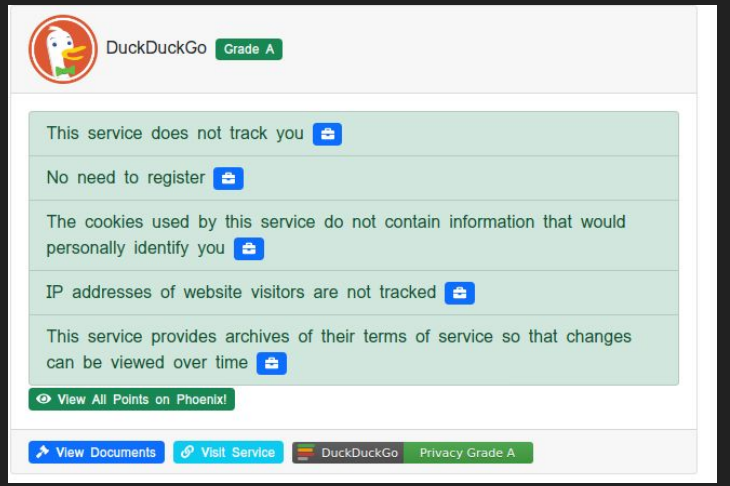
- Si c’est gratuit, vous êtes le produit
- Éviter de conserver les configurations par défaut
  - Resserrer les paramètres de confidentialité notamment
- C’est l’affaire de tout le monde
  - Si vos amis donnent accès à l’information qu’ils ont accès sur vous à une application…
  - Fonction “Inviter vos contacts” ou “Trouver vos amis”
- Corrélation des comptes entre divers services
  - nom+siteweb@domaine.ca pour complexifier la tâche
- Séparation des comptes personnels et professionnels



https://redd.it/qemds0

- Beaucoup de services utilisent un biais cognitif pour faire passer des droits abusifs
- Un example clair:





https://tosdr.org/

La relation de confiance utilisateur/service est compromise à la racine pour certains.

Être le produit...pourquoi?

- Marketing/campagne d’influence ciblée
- Entraînement de modèles ML/IA
- Profilage
- Accumulation de métriques [pour améliorer des produits]
- Antispam
- Droits d’utilisation du contenu téléversé

Facile à oublier

- Verrouiller le téléphone
- Discussions entre amis, famille et conjoints
  - Si vous n'arrivez pas sainement à avoir ces discussions, il y a un problème
  - Vous habitez ensemble? Chercher des tests de grossesse en ligne sans en parler..?
  - Ne pas partager ne veut pas dire ne pas avoir confiance
- Vous avez une entreprise? Un NEQ?
- Il se passe quoi avec vos données lors d'un *merger*?
- Succession

OpSec vs vie privée - définitions

OPSEC = OPeration SECurity, terme à base militaire, s'applique contre toute menace: Criminels, individus, gouvernements, sociétés privées… Le monde est un moyen de compromission;

Selon le ***DOD*** :

1. Identifier les infos critiques
2. Identifier les menaces
3. Analyser les vulnérabilités
4. Répondre aux risques
5. Appliquer des contre mesures

OpSec vs vie privée - définitions

Méthodologie pour la vie privée: Ne faites confiance qu'à ce que vous pouvez tester, comparer et adopter avec une meilleure compréhension des risques.

Vie privée de nos jours: Pouvoir de s'isoler, ou d'isoler des informations sur soi, afin de limiter l'influence que les autres peuvent avoir sur notre comportement.

OpSec vs vie privée - définitions

- Capacités d’attaque sont évoluées, même si sécurité globale évolue (TLS chiffre activité web, mais un site peut leaker...),
- Problème actuel est le nombre de moyens de compromission, une seule app ne va pas être dangereuse, mais associer plusieurs… créer une exposition globale.

Mot d’ordre : conteneuriser, afin de mieux maîtriser ses capacités défensives.

Attention :

- OPSEC a ses limites pour un utilisateur “moyen”, on ne peut que limiter l’exposition, pas l’empêcher.
- Limitations dans l’usabilité quotidienne, savoir faire des concessions.
- Les contres-mesures interviennent **après** analyses des risques.

Modèle de risque (*Threat model*)

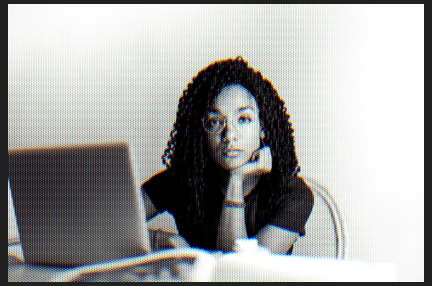
- Bâtir un modèle est un travail sur le long terme, appliquer des mesures durables demande de tester ses capacités;
- Tout modèle doit avoir capacité de changer de solution rapidement, adaptabilité fortement conseillée;

Quelques nouveautés à ce jour:

- Espace public surveillé, beaucoup de sources de données: impossible d'y échapper.
- Croisement facile depuis ces multiples sources, à considérer pour analyser ses capacités.
- Vouloir être anonyme = pas forcément utile si service garanti une forte confidentialité.

4 scénarios :

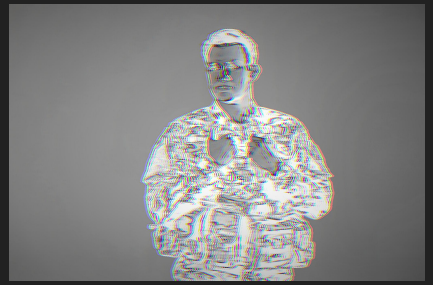
- Mère étudiante



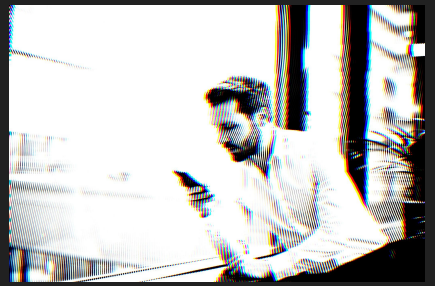
- Activiste

Possible de mélanger ces modèles

- Soldat



- CEO “control freak”



Scénarios - Activiste

- Modèle de risque **critique** (cible pour plusieurs entités);
- Doit impérativement séparer ses activités, appliquer une forme de *Zero Trust* partout (surtout en zones de repression);

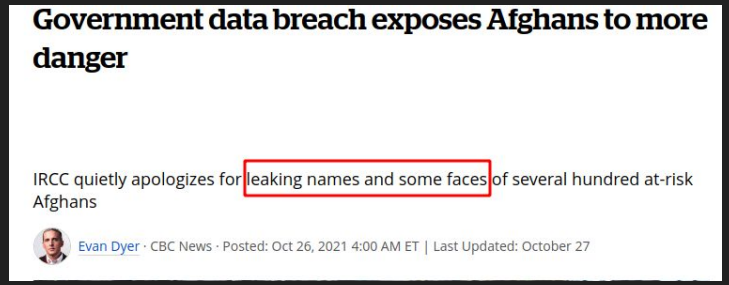
- Outils à disposition:
  - TOR (whonix/qubes)
  - machines virtuelles,
  - VPN,
  - messageries sécurisées,

- Méthodologies:
  - Contrôle à chaque étape: OS, navigateur, moteur de recherche...;
  - Séparation des activités (et *roulement* des outils);

Est une cible même en manifestation: https://www.eff.org/deeplinks/2020/06/quick-and-dirty-guide-cell-phone-surveillance-protests

Scénarios - Activiste

- Certaines données critiques ne sont pas maîtrisables, représentent un risque encore trop peu résolu.



Government data breach exposes Afghans to more danger

IRCC quietly apologizes for leaking names and some faces of several hundred at-risk Afghans

Evan Dyer · CBC News · Posted: Oct 26, 2021 4:00 AM ET | Last Updated: October 27

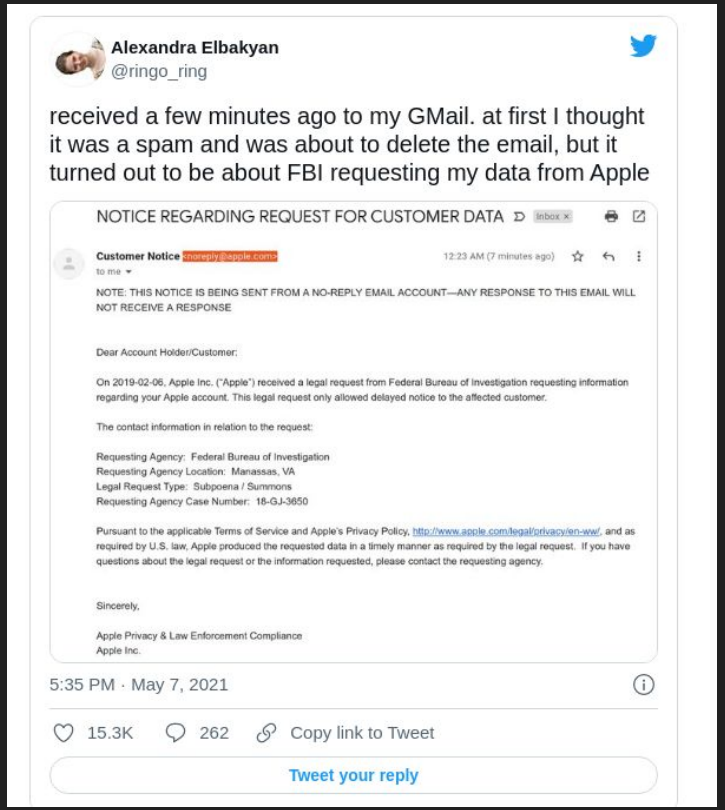
Afghanistan: Defence secretary angered over data breach

By Marie Jackson
BBC News

21 September

Données partagées par courriel... envoyées aux mauvais destinataires.

Scénarios - Activiste



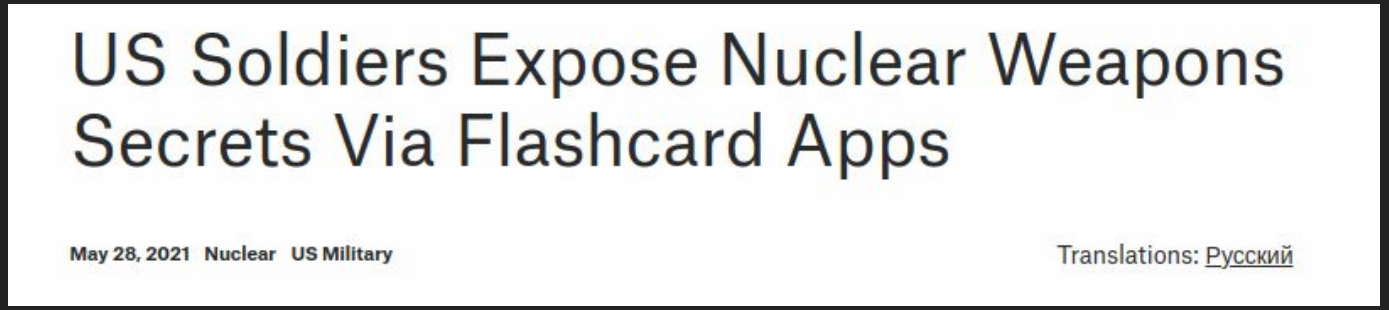
Scénarios - Soldat

- Modèle de risque **élevé :**
- Données gouvernementales sensibles, communication avec autres membres doit être sécurisé;
- Cible de la part de son propre gouvernement, et des APT étrangers;
- Conciliation entre vie privée et travail peut être complexe.

Quelques recommandations :

- Si upload des photos, utiliser un outil tel que *Fawkes* (scrap photo contre algo de reconnaissance)
- Utilisation maîtrisé des réseaux sociaux (photos, informations publiques ou privées, motif reconnaissable);
- *PilferShush Jammer (*bloque micro d'apps*),* *SnoopSnitch* (repère une possible tour IMSI) = en zone de conflit.

Scénarios - Soldat


US Soldiers Expose Nuclear Weapons Secrets Via Flashcard Apps

May 28, 2021 Nuclear US Military

Translations: Русский

https://www.bellingcat.com/news/2021/05/28/us-soldiers-expose-nuclear-weapons-secrets-via-flashcard-apps/

https://securityawareness.usalearning.gov/opsec/index.htm

Scénarios - Mère étudiante

- Modèle de risque **moyen :**
- Données de son enfant à charge (*double charge*);
- Données universitaires, bancaires, gouvernementales...
- Profil non technique, mais soucieuse de sa vie privée;

Recommendations en vrac:

- Peut utiliser des services moins gourmands (Nitter/Twitter, Invidious/YouTube, Teddit/Reddit…), ces services réduisent le tracking front-end (mais ne l'empêchent pas).
- Un gestionnaire de mot de passe apportera une forte sécurité face aux brèches de mots de passe.

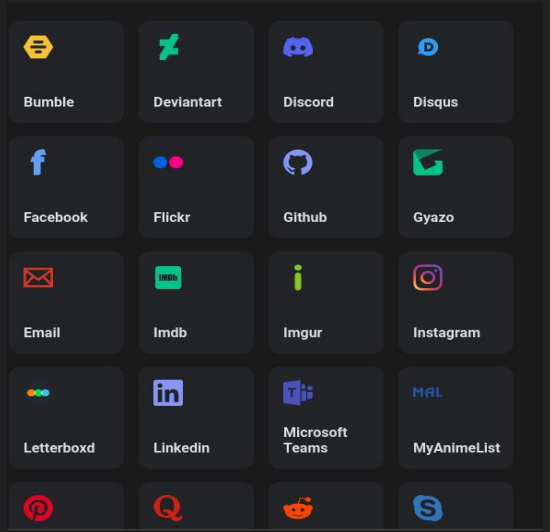
Attention particulière sur les infos partagées publiquement, aussi en privé (partager des documents par courriel, messageries non chiffrées…)

Scénarios - Mère étudiante

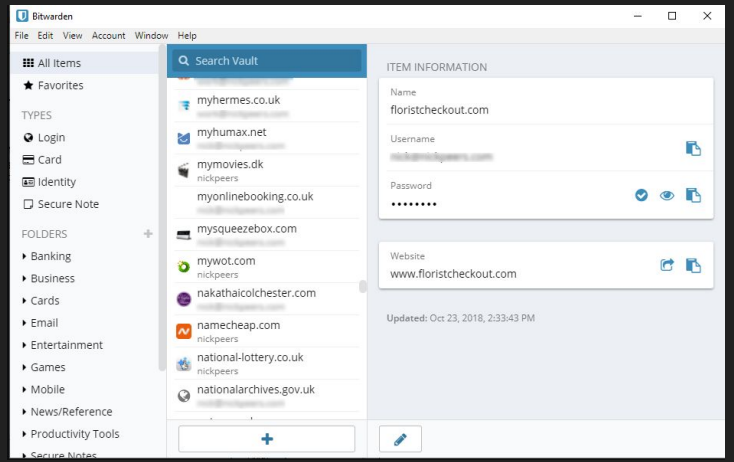
Le but est de reprendre un certain contrôle de son exposition.

Peut commencer par faire un ménage de ses réseaux sociaux:

- https://redact.dev/



- Gestionnaire de mots de passe



Les brèches

- Utilisation massive de services en lignes, brèches fréquentes;
- Avant catastrophique pour les mots de passe (moins d'actualité avec un gestionnaire):
- Le leak des données identifiables est devenu stratégique.

- Une seule info leakée n'est pas toujours dramatique.
- Plusieurs permettent une capacité d'attaque (et de fraude).

- Restreindre le partage d'infos que l'on juge critiques et pas nécessaires.
- Rester vigilant aux nouvelles.

Scénarios - CEO control freak

- Modèle de risque **sensible/critique**
- Un leak serait catastrophique, doit appliquer des correctifs partout (code, employés, outils du quotidien…);
- Mais doit utiliser des outils gourmands (Office 365, Zoho desk…) ;
- Risques d'intrusion depuis APT et employés;
- Voyage régulièrement, se rend dans plusieurs lieux (plus d'exposition);
- Forte responsabilité perso et pro.

Quelques pistes :

- Pour entreprise, intégrer un EDR et service de détection des menaces (SOC).
- Peut vérifier chambres d'hôtel, salles de réunion, surtout dans certains pays avec une législation compromise (et aussi utiliser des appareils différents).
- Privilégier la 4G/5G au WiFi public.

Scénarios - CEO control freak

- Si utilise Windows, applique une séparation entre activités perso/pro;
- Sépare différents appareils, à jours et avec un *least privilege* pour certains;
- Peut vérifier les fichiers partagés (malwares, spywares) depuis virustotal, joesandbox…
- MFA TOTP partout.

Example: Doit se connecter à un réseau public lors d'une présentation:

- Utiliser *Ooni Probe*: permet de détecter des modifications réseau (fonctionne en requêtes, pas très discret), mais un VPN sera suffisant en général.
- Éviter le *Shoulder Surfing*, surtout en public, avec un *privacy filter*.

Vecteur de compromission de vie privée/OpSec

- Pour chaque vecteur, nous mentionnons :
  - La/les problématiques associées
  - Explication des risques
  - Mitigations possibles
  - Des exemples en lien avec les scénarios sont fournis
  - Des éléments d’actualité
  - Des questionnements à se poser

Attention

- Plus on sécurise, plus on devient unique.
- Threat model critique = moins de confort d’utilisation.

Vecteur de compromission - courriels

- Utilisation du TLS : Server ou CA compromis...
- PGP crypte seulement le corps du message, pas le sujet ou le destinataire.

Solution partielle:

Utiliser *proxy emails* (simplelogin, anonaddy…) avec différents mots de passe: limite conséquences de brèches et réduit tracking entre sites.

Expérience: Utiliser nom spécifique (email.for.this.website@simplelogin.io), et repérer les usages par d'autres entreprises commerciales.

Un courriel restera toujours vulnérable, protocol limité (peu importe les promesses de certains services).

Vecteur de compromission - courriels

Le cas des courriels chiffrés: Protonmail, Tutanota, Ctemplar…

- Intérêt principal: *Zero knowledge* (boîte de réception).
- Si utilisation du même service, possibilité de chiffrement in/out
- Possèdent généralement moins d'informations personnelles,

Mais soumis aux mêmes lois que Gmail, Outlook etc.

ProtonMail deletes 'we don't log your IP' boast from website after French climate activist reportedly arrested

Sauf que : Pas d'accès au compte (législation actuelle favorable), ni au contenu des échanges (mais le destinataire pourrait être compromis de son bord).

En résumé: La différence principale réside dans les politiques anti-tracking favorisées, et le chiffrement du compte.

Vecteur de compromission - courriels

En bref:

- Un courriel restera un courriel, ne peut qu'être mitigé, pas suffisamment amélioré.

Possibilités:

- Proxy emails: A privilégier.
- Minimiser l'utilisation des courriels pour communiquer, favoriser d'autres méthodes.
- Tout comme le stockage Cloud, si l'hébergeur possède les clés, pas de garantie.

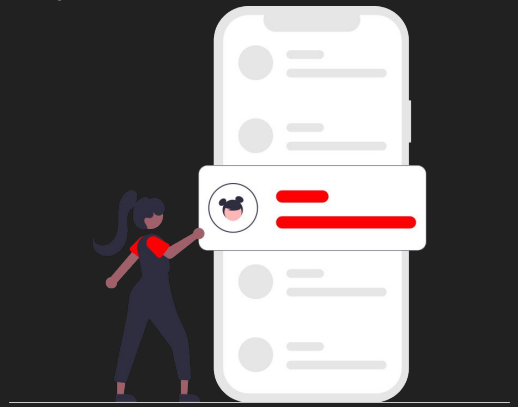
⚠️ Scénario Activiste Soldat : Aucun courriel ne garantira une confidentialité suffisante, privilégier une messagerie chiffré.

Même Secmail sous Tor peut être compromis (si mal administré).

Vecteur de compromission - messagerie instantanée

Problématiques principales à se poser :

- Financement de ?
- Modèle économique ?
- Le chiffrement est-il activé par défaut ?
- L'application et le serveur sont-ils entièrement open source ?
- L'application applique-t-elle le principe du *forward secrecy* ?
- Les informations personnelles (# de cellulaire, liste de contacts, etc.) sont-elles hachées ?
- L'application chiffre-t-elle les métadonnées ?
- Types de primitives cryptographiques ?
- L'entreprise fournit-elle un rapport de transparence ?



Une solution sûre et confidentielle dépend de :

1. Votre utilisation (ingénierie sociale, usurpations, exposition...)

2. Implémentations cryptographiques (chiffrements, normes publiques, revues etc.)

3. Pour les services, les pratiques de confidentialité (gestion ou conservation des données, politique et pratiques réelles* de confidentialité).

* Démontrées depuis plusieurs cas ou sources, sur le moyen-long terme.

Pourquoi pas WhatsApp ou Telegram?

WhatsApp:

- Code source non auditable;
- Protocol Signal, mais génère des métadonnées qui aident à la corrélation;
- Maison mère Facebook, pas de *trust*.

Telegram:

- Facilités de customisation,
- Chiffrement custom, E2EE pas activé par défaut,
- Financement “douteux” par le passé.

Vecteur de compromission - messagerie instantanée

Pourquoi pas WhatsApp ou Telegram?

https://threatpost.com/telegram-toxiceye-malware/165543/

Étude d’alternatives : Signal

- Bonne politique de confidentialité, pratiques E2EE; code open source;
- Le protocole de signal est reconnu publiquement, ne fais pas “confiance” aux serveurs;
- Fonctionnalité *sealed sender* (vérification de la session);
- Pas d'historique de chat, les *prekeys* sont renouvelées (évite *replay attacks)*,
- Appels video chiffrés;
- Les clés ne fonctionnent que sur les nouveaux messages à venir,
- Historique auditable.

Nécessite un numéro de cell (mais VOIP accepté).

Bon pour :

- Tous scénarios, car facile d’utilisation et actuellement fiable.
  - Si un numéro de cell est critique, potentiellement pas adapté.

Les métadonnées sur Signal

Preuve concrète des données recueillies :

1. "Account and Subscriber Information"

Account	Responsive Information in Signal's Possession
[redacted]	Last connection date:1607904000000 Unix millis Account created:1598050513722 Unix millis
[redacted]	Last connection date:1600214400000 Unix millis Account created:1588294832436 Unix millis
[redacted]	Last connection date:1600300800000 Unix millis Account created:1598075941655 Unix millis
[redacted]	Last connection date:1600300800000 Unix millis Account created:1598670285442 Unix millis
[redacted]	Last connection date:1608076800000 Unix millis Account created:1588035489668 Unix millis
[redacted]	Last connection date:1599955200000 Unix millis Account created:1594131337100 Unix millis

https://signal.org/bigbrother/central-california-grand-jury/

Même si Signal accepte de répondre aux requêtes légales, ne peut donner de l'info identifiable.

- Faire confiance au protocole plutôt qu'aux promesses de la politique de confidentialité .

Étude d’alternatives : Briar

Bon pour : Activiste, soldat, Chef d’entreprise.

- Messagerie chiffrée de pair à pair (Tor, WiFi, Bluetooth…),
- Messages stockés sur l’appareil (pas de cloud),
- Messages, audio, vidéo,
- Le destinataire doit être en ligne pour recevoir un message,

Le format d’utilisateur est très peu identifiable:

briar://amv’**********nv0dvr

Briar est décentralisé, pouvant convenir pour certaines préférences.

En conclusion

- Plusieurs choix, mais plusieurs points à prendre en compte:
  - https://www.securemessagingapps.com/

- Les communications sont critiques, rester vigilant :

Anom: Like WhatsApp for criminals, but secretly owned by the FBI

Global sting operation has resulted vast drugs seizures – that's the tip of the iceberg

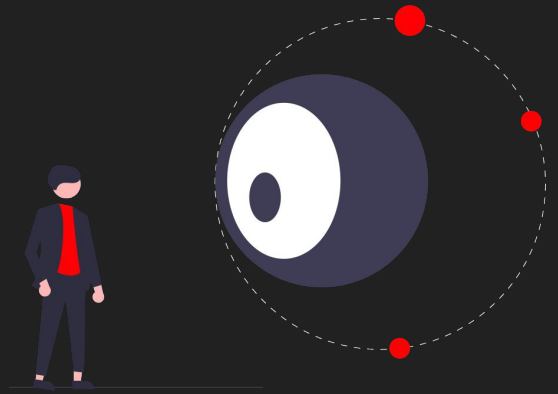
Wed, Jun 9, 2021, 10:29 | Updated: Wed, Jun 9, 2021, 10:30

https://www.irishtimes.com/news/crime-and-law/anom-like-whatsapp-for-criminals-but-secretly-owned-by-the-fbi-1.4588391

Vecteur de compromission - Navigation internet

- Plusieurs entités à protéger :

1. Navigateur (Chromium? *Anti tracking features*?)
2. Moteur de recherche (logs enregistrés?)
3. Comment le navigateur interagit avec le web?



Trackers

- Trackers font partie du modèle web centralisé (impossible d'y échapper complètement): type de navigateur, timezone, CPU, GPU, niveau de batterie, addons, OS …
- Trackers assignent un ID à chaque info pour regroupement depuis certains cookies ou scripts:
  - Courriel utilisé dans un formulaire sera comparé au fingerprint du navigateur, et regroupé à un ID plus ciblé etc.
- Trackers sont : des **Cookies** (données stockées dans le navigateur), **Fingerprinting** (infos sur le navigateurs prélevées), **Web beacons** (objets invisibles intégrés dans une page web = pixels trackers)

- EX: Télémétrie Office: teams-events-data.trafficmanager.net

Modèle de menace (threat model) :

1. Data brokers, sociétés de publicités…
2. *Super cookies* souvent indétectables,
3. Acteurs malveillants du web (très vaste).

Les Add-ons

Failles :

- Plusieurs failles de sécurité récentes proviennent des addons (Wordpress, Chrome…);
- Peu auditées indépendamment par le navigateur en question;
- Permissions: Accès à l'historique, cookies, données de navigation et même de modifier le code des pages auxquelles vous accédez;
- Préférable d'avoir que des addons essentiels (limite le profilage comportemental);

Capacités :

- Créer des associations d'addons qui renforcent la défense du navigateur (blocage scripts, trackers...);
- Limiter les données personnelles exposées et identifiables ;
- Accélérer certaines pages;

Associés au « Firefox tweaks », certains addons apportent un filtrage supplémentaire.

Une combinaison effective

Ublock

Bloque certains scripts, trackers ou images

Privacy Badger

Bloque trackers invisibles, widgets...

ClearURL

Supprime les éléments de tracking d'un URL

Conteneurise l'activité avec *Firefox containers*

HTTPS Everywhere n'est pas mentionné, devenu feature native des navigateurs.

Méthodes avancées

- Utiliser plusieurs navigateurs pour plusieurs utilisations, en créant plusieurs profils potentiels.
- Désactiver les fonctions inutiles (WebRTC, javascript…)
- FIREFOX: Ajouter *tweaks* racines (https://privacyguides.org/browsers)
- Sandbox le navigateur avec Apparmor, firejail… si l'on craint un fort vecteur de compromission

Méthodes avancées: Un VPN ?

- Un VPN est juste la transmission d'une confiance autrefois vers un ISP, et maintenant vers une partie tierce;
- Utiliser avec précaution, pour des tâches quotidiennes dont on souhaite éviter une possible exposition de son opérateur;
- Favoriser un fournisseur transparent sur plusieurs aspects:
  - Audits publiques, politique de confidentialité **claire,** rapports réguliers sur l' état de sécurité;
  - Certains proposent même une section indiquant si la plateforme est compromise.

⚠️ Scénario Activiste Soldat : Un VPN peut ne pas répondre complètement à leurs attentes, mais reste un outil stratégique. En minimisant certaines infos (paiement, courriel…) lors de l'inscription, on réduit des risques communs.

Méthodes avancées: Un VPN ?

Beaucoup de moyens pour des VPN non ?

https://restoreprivacy.com/kape-technologies-owns-expressvpn-cyberghost-pia-zenmate-vpn-review-sites/

Kape Technologies

purchases CyberGhost VPN for $10 million

ExpressVPN for $936 million

Zenmate VPN for $5 million

Private Internet Access for $127 million

Conclusion

- La sécurité et la confidentialité dépend à majorité de votre comportement, les outils techniques ne sont là que pour aider;
- Bloquer des trackers ou scripts fait en sorte que plusieurs sites ne marchent plus, mais améliore la défense;
- Les plugins doivent êtres pris avec précaution, car ils rendent la navigation plus unique, et peuvent êtres vecteurs de failles;
- Il ne manque pas de points d’informations pour vous identifier;
- Il n’y a pas de solution ultime, il en faut plusieurs, qui sont adaptables.

Vecteur de compromission - appareils mobiles/IoT

GSM:

- Communications voyagent en clair, les appels aussi.
- Relativement bon marché et simple à déployer, toujours massivement utilisé.

Multiples vulnérabilités: SIM card tracking (ICCID), IMEI tracking (numéro de serie), SMS (non chiffré), IMSI tracking (catchers & Stingrays), MSISDN tracking (numéro de cell), sim snooping, spoof calls (appels frauduleux)...

Mauvaise méthode de 2FA !
(pourtant seule option chez de nombreux organismes)

Un SMS/appel restera toujours vulnérable, n'a pas été pensé pour la sécurité.

Vecteur de compromission - appareils mobiles/IoT

Une solution expérimentale:

- PGPP = Pretty Good Phone Privacy;
- App/feature génère tokens non identifiables pour l'échanger à la tour IMSI (ne leak pas de metadonnée);
- Compromis pour les opérateurs qui mettent du temps à améliorer la sécurité/confidentialité;
- Mais demande une implémentation native à chaque opérateur (doit être déployé en masse).

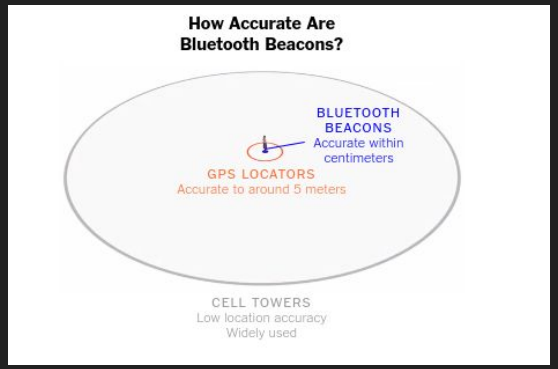
Possibilités actuelles:

- VoIP : enlève certaines failles d'une carte SIM, et peut être moins invasive pour certains (activiste);
- Carte SIM prépayée: Mint mobile et autres qui permettent de recharger son compte depuis un moyen de paiement type cash.

Vecteur de compromission - appareils mobiles/IoT

2. Appareils:

WiFi/Bluetooth (diffusent les noms de points d'accès dont il se souviennent à chaque fois qu'ils recherchent un réseau), option désactivable;



https://www.nytimes.com/

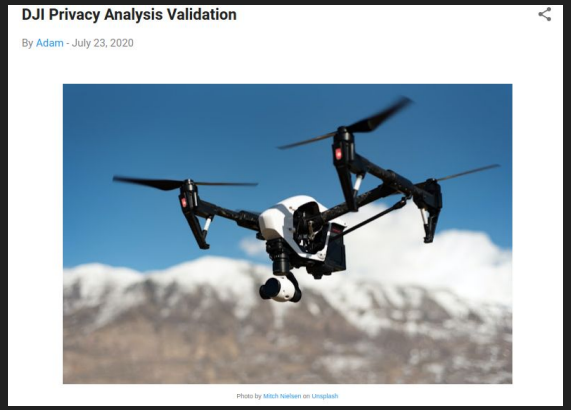
- Même en OFF, BLE peut être accessible par des communications proches.
- Souvent utilisé à des fins de marketing, sans autorisation au préalable.

- Plus on utilise d’appareils connectés, plus on ouvre les possibilités à un usage abusif.
- Un premier pas est de limiter ces appareils, bien qu’on ne puisse éviter totalement une pratique externe (centres d’achats, lieux publiques…).

Vecteur de compromission - appareils mobiles/IoT

3.IoT

- Tout objet connecté peut être détourné de sa fonction (Apple AirTags = tracking);
- Obscurité dans le développement - on ne connaît pas le fonctionnement…
- Moins d’updates que pour des logiciels classiques;



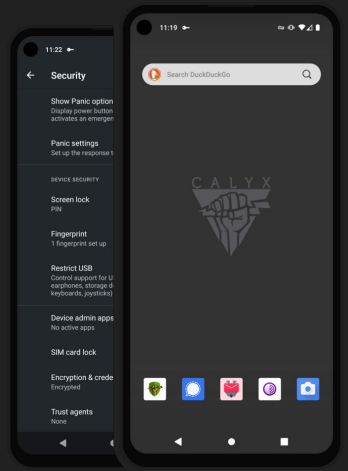
“Avant la version 4.3.36, l'application contenait le SDK Mob, qui collecte les informations privées de l'utilisateur et les transmettait à MobTech, une société d'analyse chinoise.”

https://blog.grimm-co.com/2020/07/dji-privacy-analysis-validation.html

Étude d’alternatives : CalyxOS / GrapheneOS

ROM alternatifs:

- Plus de fonctions de sécurité (et vie privée), moins impactés par le tracking Google;
- Play store remplacé par F-Droid (open source), mais possible d’utiliser apps propriétaires (aurora store), avec microg (librairie *google play services* alternative);
- Updates explicatives (changelog disponible).
- Possibilités de *sandbox* des apps gourmandes.



Peu de compromis, mais seulement sur famille Pixel.

Étude d’alternatives : CalyxOS / GrapheneOS

ROM alternatifs:

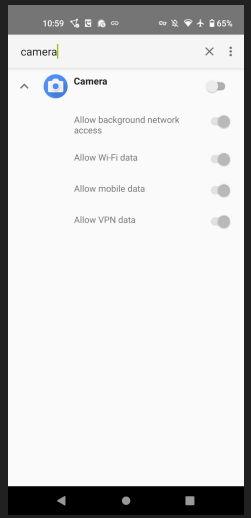
- CalyxOS permet les *push notifications*, adapté pour le quotidien (+ communauté active sur certains réseaux);
- GrapheneOS est parfois limité pour un public moins exigeant, mais planche sur un système de *push notifications*;
- Combinés à une utilisation restreinte d’applications invasives, ces ROM sont des alternatives durables.

Mythe commun : Le mode avion désactive la plupart des radios de l'appareil (signal de l'opérateur, Bluetooth, Wi-Fi) mais pas le NFC ou le GPS.

Ces ROM apportent une protection racine, mais ne changent le modèle GSM.

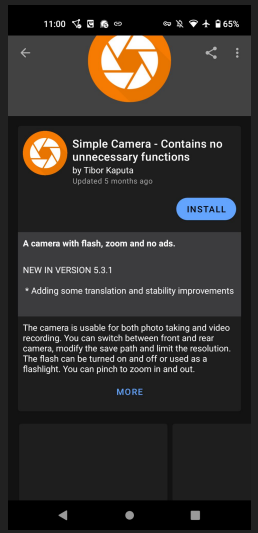
Vecteur de compromission - caméras et micros

- Assumer que toute app demandant la permission camera/micro peut l'utiliser à des fins frauduleuses;
- Plus l'app a de services (filtres, retouches…), plus les 3rd parties communiquent avec l'appareil.



Bloquer l'accès au réseau depuis le firewall (*Datura* sur CalyxOS)

Utiliser une app open source (*Simple Camera*)



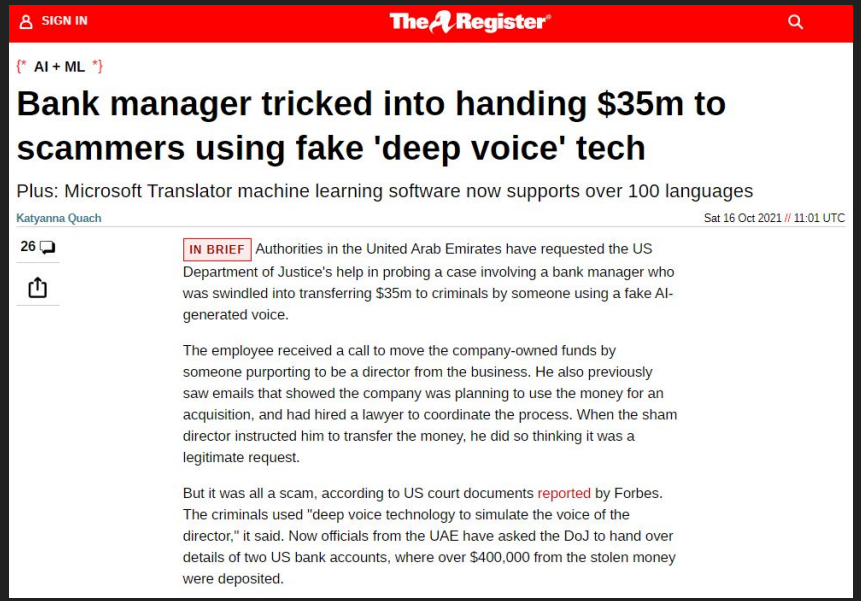
Vecteur de compromission - caméras

Recommendations générales:

- Possible de chiffrer ses photos (*Cryptocam*), mais lecture impossible sur l'appareil (besoin d'un logiciel PC);
- Par précaution, la suppression des EXIF est recommandée si on laisse les permissions de géolocalisation sur l'application (ScrambledExif);
- Un outil comme *Fawkes* aide à limiter la reconnaissance faciale sur des images mises en publique ou privé;
- Reconnaissance des lieux par OSINT est parfois un jeu, mais peut devenir un risque si on ne le souhaite pas.
    - Faisable aussi par technique de *feature extraction* et prédiction (reco faciale).

- Assumer que chaque photo sur Internet est un vecteur de compromission.
- Ce risque est une composante majeure de l'hygiène numérique, et critique en fonction du modèle de menace.

Vecteur de compromission - micros



SIGN IN

The Register

{* AI + ML *}

Bank manager tricked into handing $35m to scammers using fake 'deep voice' tech

Plus: Microsoft Translator machine learning software now supports over 100 languages

Katyanna Quach

Sat 16 Oct 2021 // 11:01 UTC

26

IN BRIEF Authorities in the United Arab Emirates have requested the US Department of Justice's help in probing a case involving a bank manager who was swindled into transferring $35m to criminals by someone using a fake AI-generated voice.

The employee received a call to move the company-owned funds by someone purporting to be a director from the business. He also previously saw emails that showed the company was planning to use the money for an acquisition, and had hired a lawyer to coordinate the process. When the sham director instructed him to transfer the money, he did so thinking it was a legitimate request.

But it was all a scam, according to US court documents reported by Forbes. The criminals used "deep voice technology to simulate the voice of the director," it said. Now officials from the UAE have asked the DoJ to hand over details of two US bank accounts, where over $400,000 from the stolen money were deposited.

Phishing on steroid

Google & Samsung fix Android spying flaw. Other makers may still be vulnerable

Camera and mic could be controlled by any app, no permission required.

DAN GOODIN - 11/19/2019, 12:32 PM

- Moins d'applications "inutiles", moins de risques;
- Si modèle critique, enlever le micro ou le restreindre depuis une app de gestion reconnue.

Vecteur de compromission - applications

- Apps contiennent des *call backs* invisibles en plus de permissions privilégiées;
- Préférer des alternatives open source et auditables au possible;
- Éviter d'utiliser un compte perso Google/Apple (et randomiser des infos que l'on ne souhaite pas publiques);
- Une app comme *Vigilante* prévient de l'utilisation d'un micro, caméra ou enregistrement par une application.

- Utiliser un firewall ou bloqueur (*Blockada*) afin de filtrer les requêtes;
- Recommandé de filtrer ces bloqueurs à la racine du réseau (depuis un firewall) ou avec un piHole (DNS!) correctement configuré.

Attention aux faux positifs, demande du tuning au début.

Vecteur de compromission - outils de collaboration

- MS Teams, Hangouts, Slack… Pas E2EE;
- Zoom a menti par le passé:

Zoom lied to users about end-to-end encryption for years, FTC says

- Intègrent souvent des services tiers (*Confluence, Jira*) qui partagent de la télémétrie;
- Certaines alternatives gratuites/open source suffisent, mais seront moins complètes que les principaux concurrents (Jami/Jisti Meet…).

Vecteur de compromission - Outils de collaboration

Petit point sur Matrix/Element :

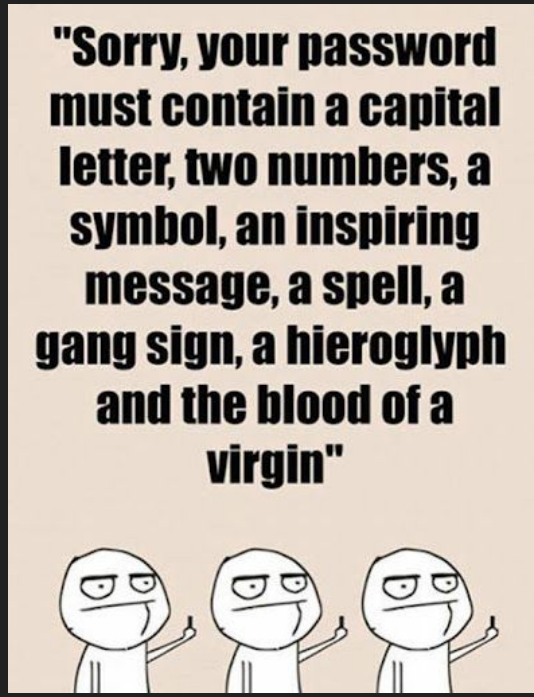
- Alternative à Slack, Discord…
- Modèle décentralisé et fédéré si souhaité;
- E2EE avec Element (mais pas par défaut)
- Génère quelques métadonnées (mais signup sans courriel, cellulaire…)

Vecteur de compromission - cartes de points et de $

- Permet aux compagnies de vous offrir de la publicité plus ciblée
- Pléthore de points de données pour vous profiler
  - Accès aux détails de vos achats
- Demandent votre adresse et autres infos
- Avantages valent-ils l’impact sur modèle de risque?
- Peuvent-ils transférer/revendre votre info?
  - Consulter EULA/contrat

Vecteur de compromission - mots de passe

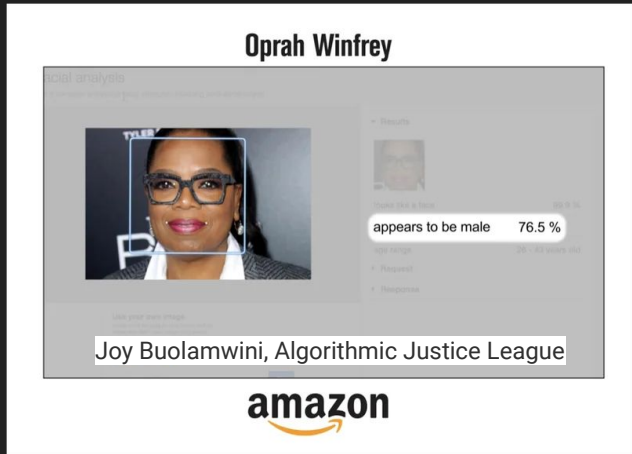
- Ils peuvent fuiter - haveibeenpwned
  - Questions/réponses secrètes - Adobe leak
- Informations intéressantes
  - Nom des enfants ou des animaux
  - Date/année de naissance
  - *Patterns*, habitudes et...réutilisation!
  - ...infos utilisées pour des questions secrètes!
- Gestionnaire de mots de passe, bonne idée!
  - Aussi pour question/réponse secrète
- 2-factor auth, une excellente pratique
  - Mais si vous prenez FidoAlexis20180320 et que ça fuite…
  - Ne pas oublier *backup codes* rangés à un endroit sécuritaire séparé des MDP



Potentiel des données - IA & *machine learning*

- Source des données - acquises éthiquement/légalement?
- Biais - dépend des données et des modèles programmés..et des analystes
- Déanonymisation - fausse bonne idée
  - Recroisement via d'autres sources de données - inférence
- Buzzwords - Powerpoint vs Python scripts
- Impacts de l'automatisation de processus "humains"
  - Capacité de traitement + accessibilités décuplées
  - Expansion des risques connus
- Couteau à double-tranchant
- Augmentation du flou d'imputabilité

https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf



PL64

- La loi actuelle (LPRPSP) date de 1994
- “RGPD québécois”
- Mesures principales
  - Imputabilité - désigner un responsable [des processus] de la protection de l’information
  - Mise en place de politiques de protection des renseignements personnels - anonymisation
  - Écosystème de gestion et transparence du consentement des utilisateurs
  - Obligation d’avis d’incident à la Commission d’accès à l’information, et les usagers concernés
- Anonymisation - souvent trompeur et réversible
- Amendes prévues
- Entrée en vigueur s’échelonne sur 3 ans

Rétention des données

- Géolocalisation
- Données de recherche
- Historique d’achat
- Ce qu’on a mis en ligne sur nous
  - Bon de régulièrement s’auto-chercher pour éviter des surprises
- Journaux de conversations, styles d’écriture, *nicknames…*

Keep your Location History? Decide by April 1, 2022

Inbox ×

Google Location History <location-history-noreply@google.com>
to me

Hi vn,

Location History is paused for your account, and you haven't had any new Location History in more than 5 years.

Any existing Location History you have in your account will be deleted on April 1, 2022.

Here's what you can do before April 1, 2022:

- Keep this data in your account by turning on Location History in Activity controls
- Download a copy of this data before it's deleted on April 1, 2022

Autres réalités

- Changement de gouvernement/régime
- Acquisition/*merger* du propriétaire/fournisseur du service
- Différences de cultures
  - Ex: e-Tazkira en Afghanistan, Aadhar en Inde
- Guerres
- Liberté d’expression et d’association
  - S’applique à tout type d’”étiquetage” social
- Contre-espionnage


Technology

Huawei tested AI software that could recognize Uighur minorities and alert police, report says

An internal report claims the face-scanning system could trigger a ‘Uighur alarm,’ sparking concerns that the software could help fuel China’s crackdown on the mostly Muslim minority group

https://teachprivacy.com/10-reasons-privacy-matters/

Impact sur la santé mentale?

- Stress lié au sentiment de contrôle de notre vie
  - Tels les changements climatiques, problématique récente et peu connue
- Préservation de notre identité et de nos limites
- Récupérer d'un préjudice
  - Harcèlement
- Anxiété, dépression, PTSD…
- Sentiment d'impuissance personnelle vs compagnies et régulations
  - Confiance vs sécurité

Résumons: Réponses aux questions

- Prendre une photo avec un cellulaire à la base, est-ce problématique en termes de vie privée? Ou faut-il être dans une application?

➔ *Oui, c'est un vecteur car métadonnées et reliés à des parties tierces (réduire en bloquant la connexion depuis le firewall)*

- Je discutais d'un sujet chez moi avec des amis et peu après, je me fais offrir des publicités à ce sujet alors que je n'avais pas mon cellulaire. Suis-je paranoïaque?

➔ *Pas nécessairement, mais Alexa/Google ont admis écouter conversations. Seule solution est de ne pas utiliser ces devices always connected*

Réponses aux questions populaires

- Qu'est-ce qui est le pire, utiliser une plateforme qui nous track via leur site Web dans notre navigateur, ou via leur application mobile?
  - ➔ *La navigation mobile dépend de facteurs moins contrôlables (notamment des apps pré bundlées), alors que le web permet un travail d'anti tracking.*

- Je pense que mon chum m'espionne, je fais quoi?
  - ➔ *Facile d'assumer le pire*
  - ➔ *Valider connexion sur comptes*
  - ➔ *Tenter de comprendre comment/quand c'est arrivé*

Références populaires

- Films
  - The Great Hack, sur Netflix
  - The Social Dilemma, sur Netflix
  - Anon (2018)
- Série
  - Mr. Robot
- Livres
  - “On vous voit” de Crypto Québec (un autre sort l’an prochain!)
  - 1984 de George Orwell

Mots de fermeture

- À vous de trouver votre balance
- On peut donc maîtriser une partie de ses données, en s’adaptant régulièrement, mais en ayant une base solide.
- La meilleure défense est celle que l’on développe constamment, avec une évaluation pragmatique des menaces.
- Venez en discuter sur #vie-privée sur Discord
    - Si ça suit votre modèle de risque… *wink*

DISCORD

https://discord.gg/hackfest

https://discord.hackfest.ca

Podcast international sur la sécurité et le hacking. Nouvelles et opinions du Québec et de l'Europe!

https://securite.fm

InfosecJobs

https://infosecjobs.ca


HACKFEST.ca
GET
INVOLVED
info@hackfest.ca


HACKFEST.ca
Hackfest 13 - Novembre 2021
https://hackfest.ca
CONFÉRENCES & CTF: 19-20 NOVEMBRE
FORMATIONS: 14-18 NOVEMBRE
INSCRIPTIONS
FORMATIONS : EN LIGNE
ÉVÉNEMENT/CTF : BIENTÔT