# Conseils d'hygiène numérique pour honnêtes gens

Michael Opdenacker
Lycée de l’Arc, Orange
3 septembre 2024

# Michael Opdenacker

- Ingénieur informaticien indépendant
- Spécialiste en informatique embarquée et en logiciels libres
- Pas un spécialiste en sécurité informatique. Juste intéressé par le sujet.
- Présentation donnée à titre bénévole
- Habitant à Orange

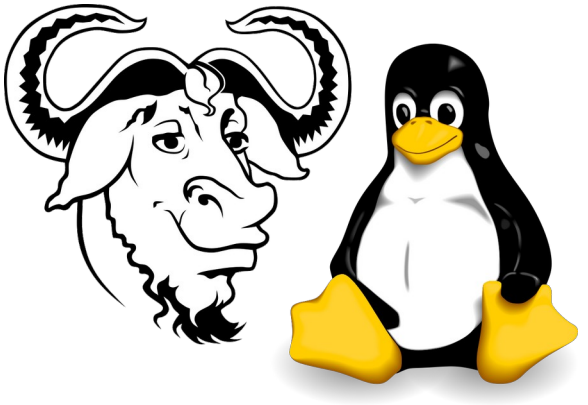


Image : https://fr.wikipedia.org/wiki/Linux#/media/Fichier:GNU_and_Tux.svg

# Pourquoi faire ?

- Éviter les fraudes
- Éviter l'usurpation d'identité
- Préserver votre anonymat, votre vie privée
- Éviter le vol et la destruction de vos données

# Quels moyens ?

- Protéger vos informations personnelles et celles de vos contacts
- Protéger votre ordinateur, votre smartphone et les données qu'ils contiennent
- Que faire en cas d’attaque ?
- Améliorer vos pratiques et la pérennité de vos données

# A propos de cette présentation

- Cette présentation est volontairement peu structurée
- Elle mélange un peu dans le désordre les différents concepts et conseils.
- C’est pour éviter la monotonie et revenir régulièrement sur certains thèmes.
- Je n’applique pas toujours bien tous mes conseils, mais ça me fait une bonne piqûre de rappel.


Image : https://upload.wikimedia.org/wikipedia/commons/2/28/Two_Cows_-_Alps%2C_Italy_-_About_1994_01.jpg
If something is free
You are not the
customer
You are the product
Merci à Tristan Nitot pour l’idée !

# Vos données ont beaucoup de valeur

- Pour vendre des publicités ciblées
- Pour vous escroquer
- Pour vous rançonner
- Pour vous surveiller
- Pour faire appliquer la loi

# Exemples de données

- Nom et prénom
- Date de naissance
- Lieu de naissance
- Adresse
- Employeur
- Positions GPS et horaires
- Contacts
- Performances sportives (montre connectée)
- Données de santé
- Justificatifs de domicile
- Recherches sur Internet
- Réactions sur réseaux sociaux
- Articles et media sur réseaux sociaux
- Messages échangés
- Commandes sur Internet
- Musique, films ou applications
- Fichiers personnels ou professionnels
- Codes d’accès personnels

La réglementation européenne établit des droits et des devoirs autour des données personnelles (RGPD) : https://fr.wikipedia.org/wiki/Règlement_général_sur_la_protection_des_données

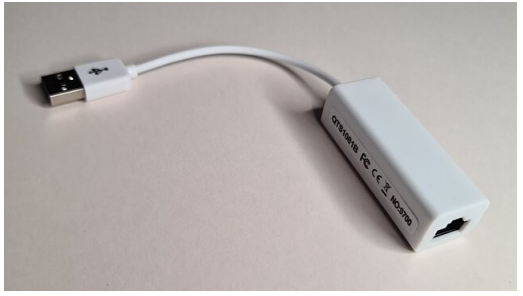
# Vous trouvez une clé USB...

- Est-ce que vous la branchez pour voir ce qu’il y a dedans ?
- Non ! 😱

Image : https://hak5.org/products/omg-plug

# Vous trouvez une clé USB...





Qui n’est pas ce que vous croyez !

Images :
https://hak5.org/products/omg-plug
https://commons.wikimedia.org

# Encore un exemple...

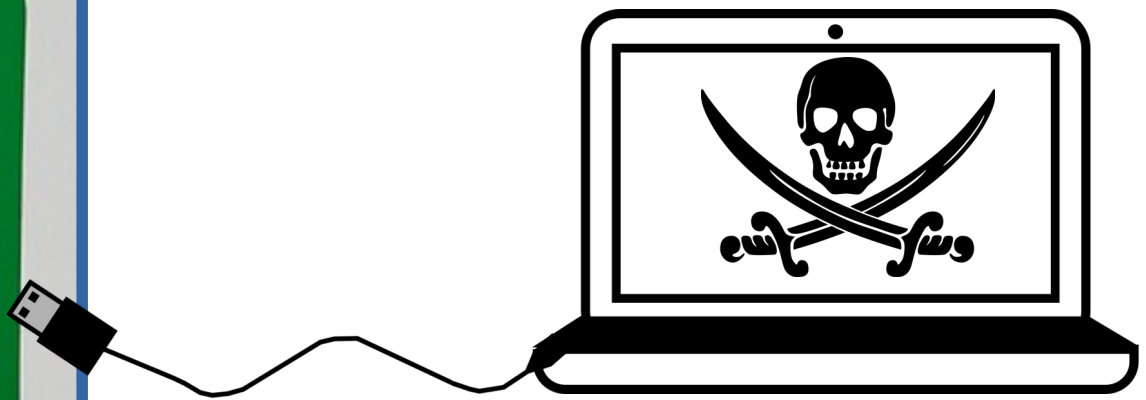
https://youtu.be/l8YpTOv7Q2A?t=27

# Vous voulez charger votre portable ?


- Vous trouvez une prise dans un lieu public.
- Ça peut être dangereux 😬

Image : https://commons.wikimedia.org/wiki/File:USB_Charging_Port_of_Jinan_Metro_Line_3_20200412.jpg

# Vous voulez charger votre portable ?

Derrière la prise, ce n’est pas un chargeur
mais un ordinateur qui peut siphonner vos données !

Images :
https://commons.wikimedia.org/wiki/File:USB_Charging_Port_of_Jinan_Metro_Line_3_20200412.jpg
https://openclipart.org

# Quelques conseils

- Ne jamais brancher une clé USB inconnue
- Éviter de charger son téléphone ou PC sur une prise publique, dans un hôtel ou sur un portable inconnu.
- Ne laissez pas quelqu'un charger sa cigarette électronique sur votre PC.
- Utiliser son propre chargeur ou un câble « no-data »


Image : https://portablepowersupplies.co.uk/product/usb-data-blocker

# USB pour griller un appareil

- Des « clés USB » peuvent envoyer des impulsions à haute tension pour « griller » un appareil (PC, téléphone, écran, prise dans un avion...).
- Tout appareil qui a un port USB devrait être protégé contre les surtensions, mais c’est encore loin d’être le cas.
- https://youtu.be/I6bRoSK39io


https://usbkill.com/

# Pour éviter l’usurpation d’identité

- Éviter le plus possible de donner des copies de vos documents d'identité et autres justificatifs de domicile.
- Quand c’est nécessaire, rajoutez un filigrane pour limiter l’utilisation à votre destinataire.
- Préférez les copies papier pour les documents sensibles.


https://filigrane.beta.gouv.fr/

# Attention à votre date de naissance

- De nombreux sites vous demandent votre date de naissance, pour en faire quoi ? 🤨
- Ne leur donnez pas, où si l’on vous force, donnez une date (légèrement) fausse.
- Idem pour les réseaux sociaux.
- La date de naissance est un élément qui peut aider à se faire passer pour vous.

# Attention à votre CV

- Pas trop d’infos personnelles sur votre CV !
- Ne gardez que le nom et l’e-mail si vous le partagez sur Internet


CV trouvé sur LinkedIn (que j’ai anonymisé)

# Permissions des applications

- Ne donnez aux applications que les permissions dont elles ont besoin.
- Attention à : localisation, contacts, fichiers, réseau…
- J’ai longtemps essayé d’utiliser WhatsApp sans donner accès à mes contacts, mais l’application ne veut pas fonctionner correctement. Normal, WhatsApp appartient à Meta (Facebook), qui veut avoir ce genre d’information !

# Attention à ChatGPT

- ChatGPT ne vous garantit pas le secret de vos conversations.
- Il peut utiliser vos informations pour alimenter ses « connaissances ».
- Ne lui soumettez pas des informations confidentielles !

# Facebook « shadow profiles »

- Attention, Facebook vous connaît même si vous n’avez pas de compte Facebook !
- En particulier grâce aux utilisateurs qui partagent leurs contacts (dont vous faites partie) avec Facebook.
- Pas grand-chose à y faire. C’est comme ça que ces réseaux sociaux devinent vos amis sans que vous ne leur ayez jamais dit.

https://www.howtogeek.com/768652/what-are-facebook-shadow-profiles-and-should-you-be-worried/

# Conseils pour les réseaux sociaux

- Il ne s'agit pas de s'en priver !
- Juste faire attention aux infos partagées.
- Ne pas donner sa (vraie) date de naissance
- Ne pas poster ses photos pendant ses vacances (les cambrioleurs savent que vous n'êtes pas chez vous)
- Ne pas publier de photos de tiers sans leur accord. Attention en particulier aux photos d'enfants, en particulier les vôtres (voir la campagne sur https://youtu.be/xrpVBuUDS1s).
- Attention aussi à la promotion d'événements auxquels vous participez.
- Attention aux photos « compromettantes » ou aux opinions trop marquées. Les recruteurs et écoles chez qui vous postulez vont vous chercher sur Internet.
- Idée : profils séparés – Un pour les proches (photos, etc), et un profil public.

# Attention aux GAFAM

- GAFAM = Google Amazon Facebook Apple Microsoft
- Ces entités essaient d’en savoir le plus possible sur vous pour vous proposer produits et publicités (et vendre celles-ci)
- Exemple :
  - Vous faites une recherche sur Amazon ou Google
  - Vous voyez ensuite plein de publicités sur des sites tiers (qui affichent des pubs Amazon ou Google) en rapport avec cette recherche. Merci aux « cookies » !
  - Je n’aime pas être profilé, je préfère les pubs ou suggestions d’articles neutres et élargir mes horizons.
  - Si vous surfez sur Internet avec un de vos amis ou proches, par les pubs qui s’affichent, ceux-ci peuvent deviner quelles recherches vous avez faites.

# Zoom sur Google

- Tout plein de services gratuits très pratiques !
- En particulier Gmail, vous êtes tout le temps connecté dans votre navigateur.
- Sur Android, vous êtes aussi toujours identifié. Pas possible d'utiliser un téléphone ou une tablette Android sans révéler son numéro de téléphone.
- Du coup, aucune de vos recherches sont anonymes 🤨
- C'est vrai aussi pour YouTube
- Google Mail lit aussi vos messages.
- Google suit la localisation de votre téléphone Android (et sait à proximité de quels commerces vous êtes passé).
- Sur Android, les serveurs de noms de Google sont utilisés. Même si vous n'utilisez pas le moteur de recherche, Google sait quels sites vous consultez.
- Google vous connaît sans doute mieux que vos proches 🤨
- Une fois de plus, attention aux services gratuits !

# Mes conseils pour utiliser Google

- Quand vous n’avez pas le choix
- Utilisez ses services en navigation privée, pour ne pas être identifié dans votre navigation normale.
- Idem pour YouTube
- Préférez le navigateur Firefox, conçu pour le respect de la vie privée. Ce n’est pas le but principal de Google Chrome.
- Préférez Waze (Google aussi) qui ne vous demande pas de vous identifier, à Google Maps pour la navigation. OsmAnd (logiciel libre à base d’OpenStreetMap) est encore mieux.

Firefox Browser

# A propos d’Apple

- Je ne parle que très peu d’Apple,
  car je n’utilise jamais leurs produits.
- Même si la sécurité des produits a plutôt bonne réputation, cette société a des pratiques très monopolistiques, et peu recommandables en termes de respect de l’environnement (obsolescence programmée) et des travailleurs (Ouïghours, etc.) de ses fournisseurs.

  https://fr.wikipedia.org/wiki/Apple#Travail_forcé

Image : http://betanews.com/2014/04/07/the-apple-myth-why-security-through-obscurity-isnt-security/

# Moteurs de recherche alternatifs

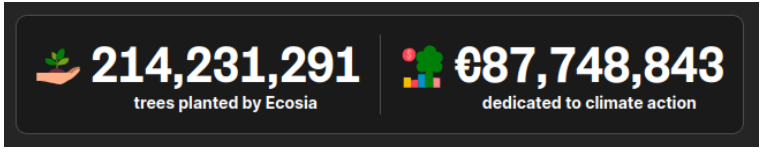
- Qwant (FR) - https://www.qwant.com/
  *Le moteur de recherche dont vous êtes l'utilisateur, pas le produit*

- DuckDuckGo (USA) - https://duckduckgo.com/

  Un méta-moteur de recherche
  *Your personal data is nobody's business.*

- Ecosia (DE) – https://ecosia.org/

  Un moteur de recherche qui plante des arbres
  *We are in it for the trees, not your data*



# Messageries alternatives

- Proton Mail (CH)
  Vos données dans un bunker
  sous la montagne dans un pays neutre
  https://proton.me/
- Tuta (DE)
  https://tuta.com/
- Posteo (DE)
  https://posteo.de/en

Des offres de base gratuites,
puis payante pour plus de volume

# Signal – Alternative à WhatsApp

https://signal.org

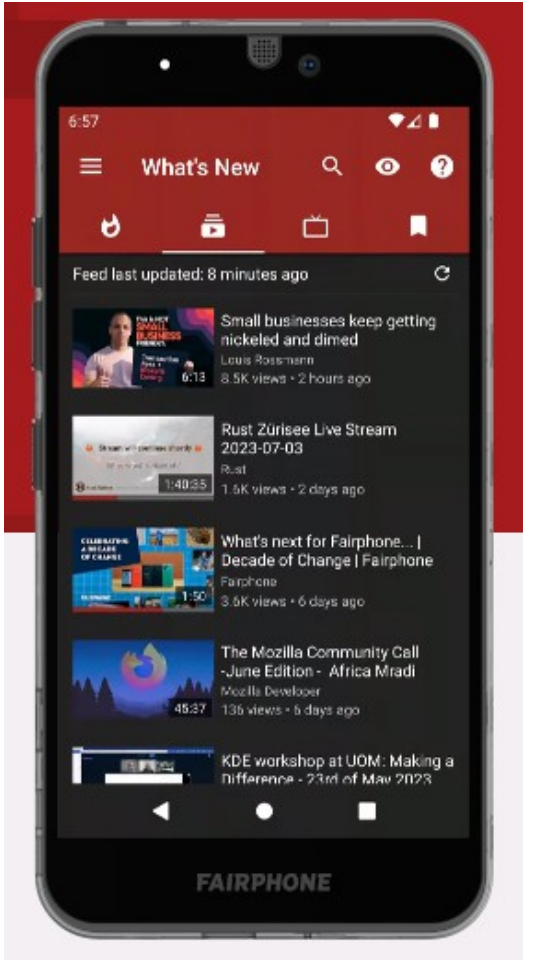
- Un logiciel complètement Open Source
- Créé par ceux qui ont créé WhatsApp après l'avoir vendu à Facebook. Financé par les fondateurs et par vos donations.
- Des fonctionnalités très complètes, voire supérieures
- Vous n'avez même pas besoin de partager votre numéro de téléphone. Un identifiant suffit.
- Telegram est utilisable aussi, mais...
  - Le serveur n'est pas Open Source,
    par défaut les messages ne sont pas chiffrés
    sur le serveur
  - Utilisé par tous types de criminels et complotistes


Images : https://signal.org/

# Newpipe

https://newpipe.net/

- Application pour Android
- Pour accéder de façon anonyme aux vidéos YouTube, et ne pas alimenter l’algorithme
- Disponible sur un magasin d’applications alternatif
- Des fonctionnalités intéressantes : téléchargements, écouter écran éteint, ne télécharger que l’audio...



# Alternatives aux services gratuits centralisés

# Mais je n’ai rien à cacher !

- Et j’habite dans un pays libre !
- L’exemple des USA et du droit à l’avortement. Problématique des historiques de location (cliniques), des recherches sur Internet et des applications de suivi des menstruations.

*Dans les Etats qui pourraient bientôt interdire l’avortement, de nombreuses traces numériques laissées par les internautes, mais aussi toute personne fournissant son aide ou des services liés à cette procédure, peuvent théoriquement être utilisées par les autorités judiciaires.*

https://www.lemonde.fr/pixels/article/2022/06/27/avortement-aux-etats-unis-les-geants-du-numerique-face-au-danger-lies-aux-donnees-personnelles_6132221_4408996.html

# Protégez votre ordinateur

- Ne jamais travailler ou surfer sur Internet en tant qu’administrateur. Trop facile de prendre le contrôle de votre machine.
- Créer un compte utilisateur pour chaque membre de votre foyer.
- Si possible, ne pas utiliser votre ordinateur professionnel pour des besoins personnels.

# Protégez vos systèmes

- Tenez vos systèmes et applications toujours à jour, pour bénéficier de correctifs pour les vulnérabilités connues.
- Téléchargez les applications depuis leurs sites et magasins officiels.
- Danger des applications piratées
- Préférez les logiciels libres (Open Source) souvent mieux sécurisées.
- Ne vous connectez pas à des réseaux Wi-Fi publics, ou alors utiliser un VPN pour sécuriser vos connexions.

# Protégez les données sur vos ordinateurs

- Chiffrez vos disques
- Y compris amovibles !
- Chiffrez vos fichiers sensibles (un pirate ayant accès à votre ordi à distance pourrait les lire)
- N’emportez pas d’ordinateurs ou de téléphones avec des données sensibles pendant des voyages à l’Étranger. Surtout dans certains pays
- Verrouillez vos sessions automatiquement
- Faites des sauvegardes, sur disques chiffrés (c'est aussi protéger ses données)
- Éteignez ou mettez en veille votre ordi quand vous ne l’utilisez pas de manière prolongée.

# Protégez votre smartphone

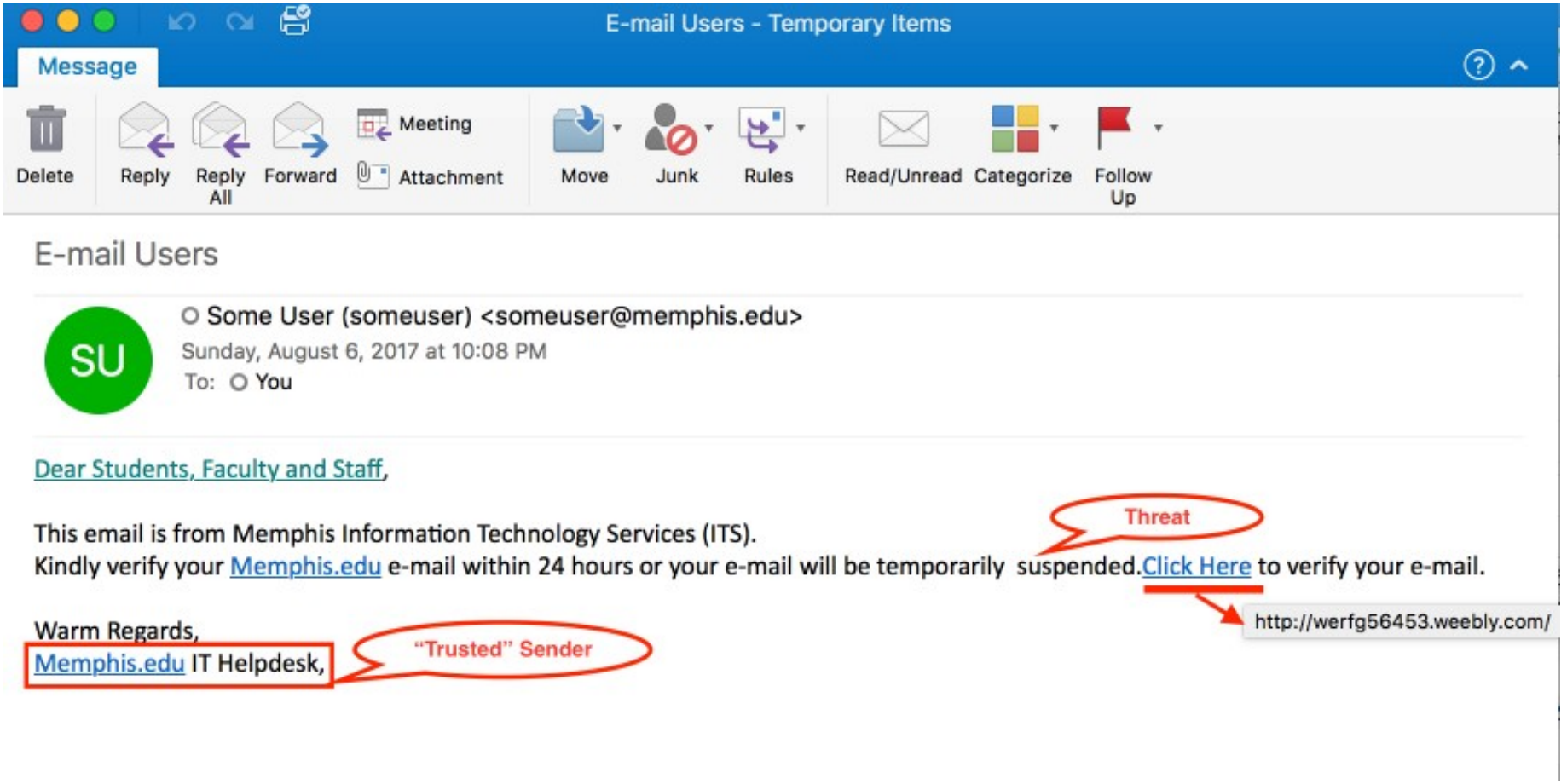
- Verrouillez efficacement votre téléphone
- Désactivez l'affichage du contenu des notifications quand l’écran est verrouillé.
- Encore une fois, ne pas le charger avec un chargeur inconnu ou alors avec un câble « no-data ».

# Évitez les fraudes

- Se méfier de tout message ou appel téléphonique où il est question d'argent ou d’urgence. Des fautes de grammaire ou d’orthographe peuvent aussi vous mettre la puce à l’oreille.
- Attention aux pièces jointes, même en provenance de vos contacts. Ne pas les ouvrir si quelque chose a l’air inhabituel.
- Attention, un courrier électronique peut être "spoofé". Idem pour les messages et appels vocaux, qui peuvent être générés par une IA, imitant parfaitement un de vos proches. Rappelez la personne en cas de doute.
- Ne pas ignorer les messages d’alerte de votre navigateur ou de votre client e-mail face à des sites ou des messages frauduleux.
- Se méfier des personnes rencontrées uniquement en ligne. De nombreux escrocs cherchent à vous piéger en ce faisant passer pour quelqu’un d’autre, et peuvent être très patients pour gagner votre confiance.

# Évitez le « Phishing »

- Éviter de suivre les liens inhabituels dans les courriels et les pages web.
- La cible du lien peut être différente de l’intitulé du lien. Bien passer la souris au dessus du lien.
- Votre client de messagerie devrait vous avertir en cas de différence.
- En cas de doute, mieux vaut taper soi-même l’adresse du site, et se connecter sans passer par le lien fourni, pour vérifier une information.




Source : https://www.memphis.edu/its/security/phishing-examples.php

# Attention au « Typosquatting »

Encore une raison de ne pas suivre les liens, ou de les taper vous-même

Quelques exemples (cherchez le piège) :

- https://support.qouv.fr
- https://support.microsoft.com

# Plus récent : le « Quishing »


Quishing = QR + Phishing

Typiquement sur parcmètres
et stations de recharge électrique

Source: https://www.20minutes.fr/high-tech/4101816-20240720-jo-paris-2024-faut-craindre-nouvelles-arnaques-faux-qr-code-pendant-jeux

# En cas d’attaque

- Si vous constatez une attaque ou un comportement suspect…
- Éteignez votre appareil immédiatement.
  Appui prolongé sur le bouton « on/off » si la batterie ou l’alimentation n’est pas amovible.
- Confiez votre appareil à un spécialiste.
- Ne pas payer les rançons si vos fichiers ont été chiffrés
- En France - déclarer l’attaque et être mis en rapport avec un prestataire pour se faire aider :
  https://www.cybermalveillance.gouv.fr/
  (accessible aussi aux particuliers)

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# Étanchéifiez vos comptes sur Internet

- Importance d’avoir un mot de passe différent sur chaque service ⚠️⚠️⚠️
- Utilisez un gestionnaire de mot de passe
- Ou stockez vos différents mots de passe de façon chiffrée sur votre ordinateur
- Si possible, utilisez aussi une adresse e-mail différente sur chaque service, pour éviter les recoupements d’informations personnelles.

# https://haveibeenpwned.com/

- Vérifier si son adresse e-mail fait partie d’une fuite de données sur Internet
- Exemple : piratage de la base de comptes utilisateur de Deezer en 2022.
- Ces données sont maintenant publiques, et peuvent servir aux pirates pour recouper les informations vous concernant, pour faire des attaques ciblées (phishing, usurpation d’identité, craquer vos comptes sur d’autres sites si vous avez utilisé le même mot de passe…)

Résultats de recherche sur mon adresse e-mail personnelle :

5 fuites répertoriées.

## Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

**Cit0day** (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

**Compromised data:** Email addresses, Passwords

**Data Enrichment Exposure From PDL Customer**: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

**Compromised data:** Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

**Deezer**: In late 2022, the music streaming service Deezer disclosed a data breach that impacted over 240M customers. The breach dated back to a mid-2019 backup exposed by a 3rd party partner which was subsequently sold and then broadly redistributed on a popular hacking forum. Impacted data included 229M unique email addresses, IP addresses, names, usernames, genders, DoBs and the geographic location of the customer.

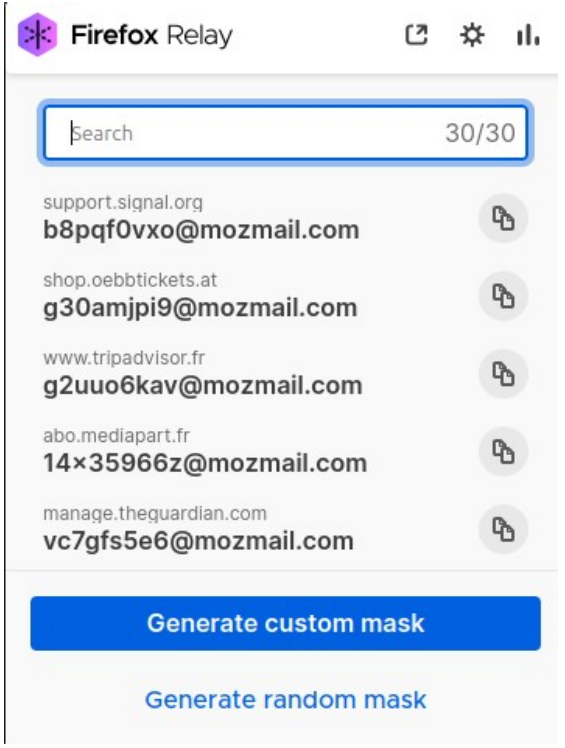
**Compromised data:** Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Names, Spoken languages, Usernames


**Pampling**: In January 2020, the online clothing retailer Pampling suffered a data breach that exposed 383k unique customer email addresses. The data was later shared on a popular hacking forum and also included names, usernames and unsalted MD5 password hashes.

**Compromised data:** Email addresses, Names, Passwords, Usernames

# Utilisez des alias d’e-mail

- Plusieurs services de messagerie offrent des alias que vous pouvez donner à la place de votre vraie adresse e-mail.
- J’utilise Firefox Relay, qui permet de gérer un alias par service. Coût : 1 EUR/mois (gratuit jusqu’à 5 alias)
- Dans certains pays, on peut même avoir des alias téléphoniques, pour garder secret son numéro de téléphone !




https://relay.firefox.com/

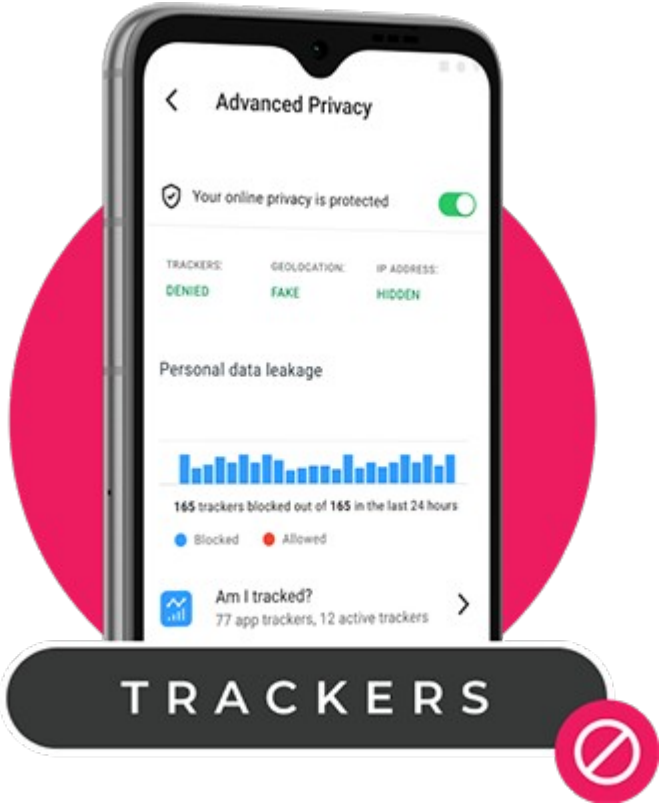
# Pour aller plus loin

- Utilisez un VPN pour que votre fournisseur d’accès à Internet (ou votre gouvernement!) ne puisse pas connaître les services auxquels vous vous connectez.
- Utilisez aussi TOR pour vous connecter de façon très difficile à tracer.
  https://fr.wikipedia.org/wiki/Tor_(réseau)
- Utilisez GNU/Linux et les logiciels libres au lieu des logiciels propriétaires. Cela vous apportera une meilleure sécurité et une meilleure pérennité pour vos données.

# /e/OS – Android dégooglisé

- Android sans Google !
  *Échapper à la surveillance numérique*
- De nombreux téléphones pris en charge
- Projet Open Source, développé par Murena.io (FR)
- Magasin d'application alternatif, bloqueur de traqueurs, masquage d'adresse IP, localisation fictive, la quasi-totalité des applications Android fonctionnent (sauf Google Maps 🤣).
- Extrêmement satisfait après presque un an d'utilisation.

https://e.foundation/fr/



# À retenir

- Partagez le moins possible d’infos personnelles
- Attention aux services gratuits, aux GAFAM
- Des alternatives existent
- Attention aux périphériques USB
- Utilisez vos propres chargeurs USB.
- Un compte pour chaque utilisateur sur votre PC
- Toujours des mots de passe différents pour les services sur Internet
- Attention à votre adresse e-mail
- Attention aux liens et aux pièces jointes
- Utiliser un système d’exploitation qui ne vous surveille pas.

# Ressources utiles

- MOOC de l’ANSSI https://secnumacademie.gouv.fr/
- Approfondir, comprendre les enjeux et se protéger
- Accessible à tous
- Durée : 6 – 10 heures

# Merci !

- Des questions ?
- Votre expérience ?
- Transparents sous licence Creative Commons Attribution – Partage à l’Identique version 4

https://gitlab.com/michaelopdenacker/digital-hygiene