Hygiène numérique

Sécurité et vie privée sur internet et appareils informatiques

Atelier proposé Medication Time

FONDATION afnic pour la solidarité numérique

Sous l'égide de Fondation de France

L'hygiène numérique?

- Une définition :
- L'hygiène est un ensemble de mesures destinées à prévenir les infections et l'apparition de maladies infectieuses.
- L'hygiène numérique, ce sont **des règles, des réflexes, des outils** destinées à utiliser son ordinateur plus sereinement et avec le plus de sécurité possible.

De quoi allons-nous parler ?

Nous allons principalement parler d'hygiène numérique dans le cadre personnel :

- sur l'ordinateur,
- durant la navigation sur internet,

l'hygiène numérique couvre d'autres domaines de nos vies numériques : mails, smartphones, objets connectées,etc...

ainsi que d'autres cadres : vie professionnelle, vie associative, etc...

et le numérique pose d'autres questions : impact environnemental, impact social et sociétal, etc...

Partie 1 : l'ordinateur

On me vole mon PC !

Quelles sont **les données que je perds** ?
> Amène la notion de sauvegarde.

Quelles sont **les données que l'on trouve** ?
> Amène la notion de chiffrement, de coffre-fort numérique.

Sauvegarde simple et efficace : Le disque dur externe

> Méthode simple : copier-coller sur un disque externe.
> Méthode plus avancé : on "synchronise" (méthode des 3-2-1 : https://www.numerama.com/cyberguerre/722952-la-regle-3-2-1-reduit-vos-risques-de-perdre-toutes-vos-donnees.html).
> On le dépose chez un·e ami·e, un·e voisin·e, un·e parent·e (pour éviter le vol, l'incendie...)

Petit plus : chiffrer le disque pour rendre son contenu inaccessible et donc pour plus de confidentialité.

Un coffre fort numérique :

https://veracrypt.fr/

Pour chiffrer un dossier, une clé usb, un disque-dur.

Les mots de passe

Temps requis pour déchiffrer un mot de passe

Traduction libre des données recueillies par Hive Systems via howsecureismypassword.net (2020)

NOMBRE DE CARACTÈRES	CHIFFRES SEULEMENT	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES	SYMBOLES, CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	1 seconde	5 secondes
7	Instantanément	Instantanément	25 secondes	1 minute	6 minutes
8	Instantanément	5 secondes	22 minutes	1 heure	8 heures
9	Instantanément	2 minutes	19 heures	3 jours	3 semaines
10	Instantanément	58 minutes	1 mois	7 mois	5 ans
11	2 secondes	1 jour	5 ans	41 ans	400 ans
12	25 secondes	3 semaines	300 ans	2000 ans	34k ans
13	4 minutes	1 an	16k années	100k ans	2M ans
14	41 minutes	51 ans	800k années	9M ans	200M ans
15	6 heures	1k ans	43M ans	600M ans	15G ans
16	2 jours	34k ans	2G ans	37G ans	1T ans
17	4 semaines	800k ans	100G ans	2T ans	93T ans
18	9 mois	23M ans	2T ans	100T ans	$7(10^{48})$ ans

Les mots de passe

Quelques règles :

> **La longueur d'un mot de passe est le facteur principal** pour créer un mot de passe solide, capable de résister à une attaque par force brute.

> Ne pas avoir le même mot de passe pour deux comptes.

> Ne pas insérer d'infos personnelles dans le mot de passe.

> Ne pas confier son mot de passe à quelqu'un d'autre.

> Passer à des phrases de passe pour les comptes les + sensibles.

https://ssd.eff.org/fr/module/cr%C3%A9er-des-mots-de-passe-robustes
https://nothing2hide.org/assets/pdf/guide-protection-numerique-2019-v3.pdf (page 4)
https://fr.wikipedia.org/wiki/Robustesse_d%27un_mot_de_passe
https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

Les mots de passe

Trop de mot de passe à retenir ?
Il existe des gestionnaires de mots de passe :

> Il y en a en ligne (Bitwarden, 1password, etc).

> Il y en a en local comme le logiciel KeepassXC (https://keepassxc.org/).

Les sites permettant de tester ses mots de passes?

> Ils sont la meilleure façon de constituer une base de données de mots de passe.
> Ne pas tester son vrai mot de passe mais un mot de passe du même type/de la même forme.
> Les mots de passe sont personnels.

Gestion des comptes sur l'ordinateur

Des comptes pour des usages différents

> Créer un compte pour chaque utilisateur·ice et un compte administrateur.
> Au quotidien, utiliser le compte utilisateur·ice.
> Le compte administrateur porte bien son nom, il ne doit servir qu'aux tâches d'administration (mises à jour et installation des logiciels...).
> Quand l'ordinateur pose une question "Je dois lancer ce programme", prendre le temps de réfléchir. Ne pas dire oui tout de suite.

Mises à jour de sécurité

FAIRE LES MISES A JOUR

> Avoir un système à jour.
> Avoir des logiciels à jour.
> Avoir un antivirus à jour.

Les logiciels ont des failles :
Une faille peut être utilisés par un programme malveillant...
Mettre à jour, c'est corriger les failles, les bugs, donc se protéger des virus, des rançongiciels, etc.

Installation de logiciels

Logiciels payants - propriétaires

Pas de logiciels crackés (le crack peut contenir un malware).
Pas de téléchargement de logiciels depuis un autre site que le site officiel de l'éditeur du logiciel. On oublie les sites 01Net, Télécharger.com (qui ajoutent des barres d'outils ou remplacent le navigateur par Chrome...).
Que les logiciels dont on a besoin (pas de démos, de logiciels Marrants...).

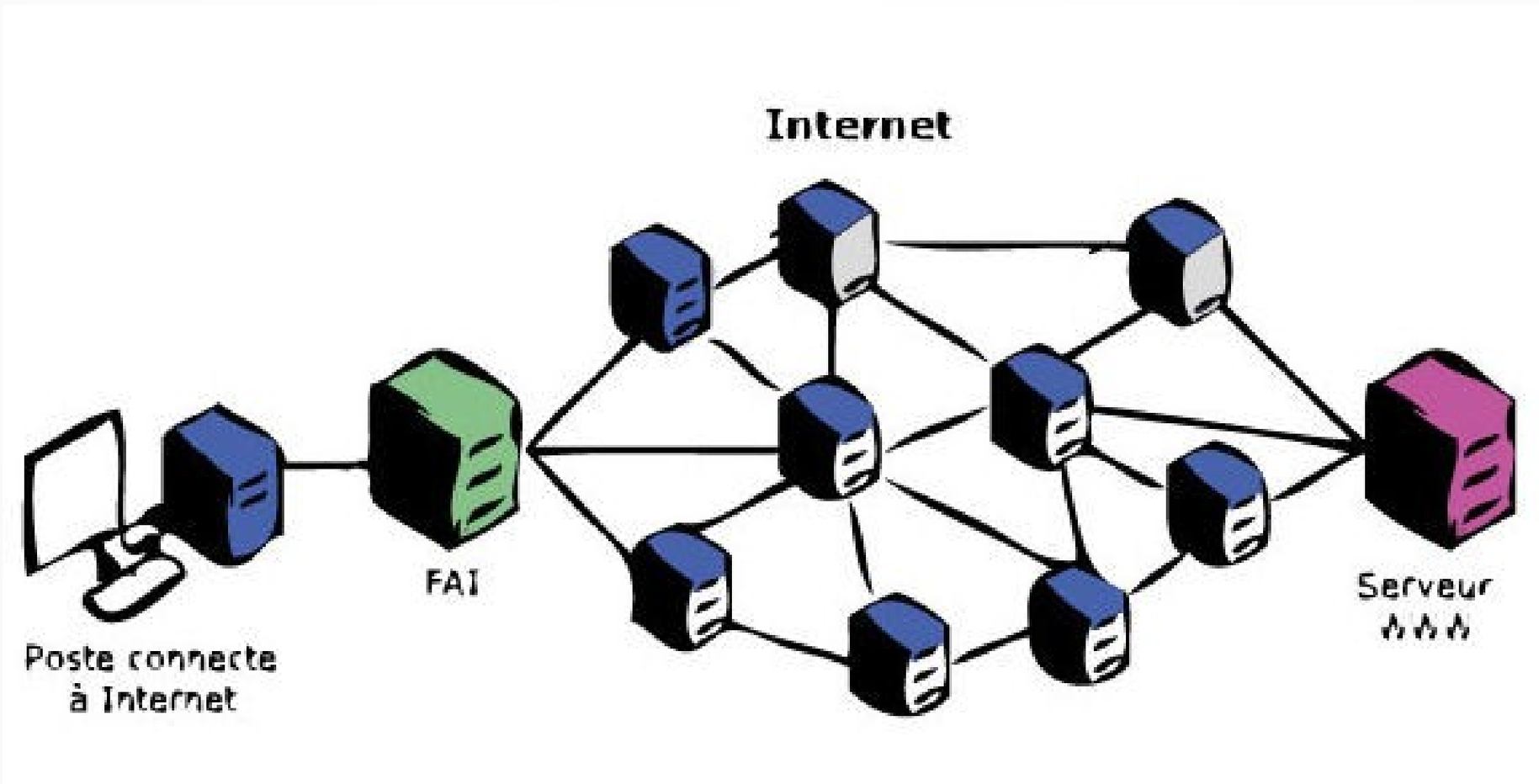
Logiciels libres

Préférer le logiciel libre - open source.
L'ouverture du code permet des audits et de combler rapidement les failles.
Passer par l'annuaire de Framasoft (https://framalibre.org/).

Attention au copain qui s'y connaît !
Ne pas le laisser installer des logiciels crackés.
Chercher à comprendre ce qu'il fait, lui demander.
S'il n'est pas capable d'expliquer, se méfier. Voire refuser.

PC = Personal Computer
Méfiez-vous de ce que l'on fait sur votre PC.
Ne pas faire confiance. Il ne faut pas prêter sa machine sans voir ce que fait l'individu à qui vous l'avez confiée.
Si prêt il faut prévoir une session invitée.
En mobilité (par exemple en train), ne pas s'éloigner de son ordi sans avoir au minimum verrouiller sa session.
Il est si facile d'installer un virus sur un PC... (avec une simple clé USB : voir clé Rubber Ducky).

Hygiène numérique & Internet



Internet, un réseau de réseau

> Internet c'est un réseau de réseaux d'ordinateurs connectés entre eux.
> Il y a les serveurs, des gros ordinateurs, sur lesquels il y a des sites Internet.
> Il y a des routeurs, qui servent à transmettre les colis que l'on appelle "des paquets".
> Il y a la Box Internet qui est (en gros) un point d'entrée et de sortie sur Internet
> Et enfin il y a notre ordinateur/tablette/smartphone...

Comment est-on pisté sur internet ?

Toutes les publicités nous espionnent

> Le **bouton Like** de Facebook : il permet à FaceBook de savoir que vous avez visité ce site, même si vous n'avez pas cliqué sur ce bouton. Même si vous vous êtes correctement déconnecté de Facebook.

> De même pour le bouton +1 de Google, les scripts de Google Analytics, les google fonts,etc...

> Toutes les publicités, Amazon...

À travers ces dispositifs ces grandes sociétés (GAFAM) récupèrent **nos (méta-)données personnelles** pour créer des profils publicitaires qu'elles revendent ensuite.
Des chercheur·ses ont nommé cela le capitalisme de surveillance.

Cloud - l'informatique dans les nuages

Définition du cloud

=

Le Cloud , c'est l'ordinateur d'un autre.

Les GAFAM

GAFAM : Google, Apple, Facebook, Amazon, Microsoft

> Concentration des acteurs d'Internet autour de silos ;
> Une centralisation nuisible (frein à l'innovation) ;
> Les utilisateur·ices de ces services ne contrôlent plus l'utilisation qui est faite de leurs données personnelles.
> Révélations Snowden (accords sur l'accès aux données entre état et entreprises du numérique, et accords inter-état https://fr.wikipedia.org/wiki/R%C3%A9v%C3%A9lations_d%27Edward_Snowden)

Sur Internet, si c'est gratuit,
c'est **VOUS** le produit

Quelques outils et réflexes pour votre navigation internet

Box internet

Votre opérateur peut observer votre activité sur internet (pas forcément le contenu mais plutôt les métadonnées).
Par défaut chaque opérateur fourni son DNS à ses abonnés qui peut être modifié pour ses besoins ou par demandes légales (DNS menteurs).
Un Domain Name Service est un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP.

Il est possible de :

- Utiliser un tunnel VPN ou le TOR browser pour sécuriser vos (méta-)données de navigation.
- Changer de DNS pour avoir un accès non-censuré à internet.

https://fr.wikipedia.org/wiki/Domain_Name_Service

Le navigateur Firefox

Logiciel open-source, code auditable.

La navigation en mode stricte

(Menu Paramètres > Vie privée et sécurité)

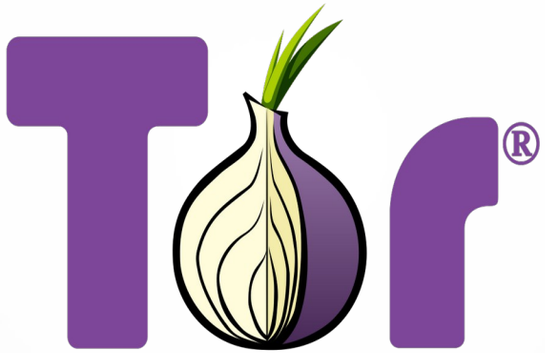
Protection renforcée, mais certains sites ou contenus peuvent ne pas fonctionner correctement.
Firefox bloque les éléments suivants :
> Traqueurs de réseaux sociaux,
> Cookies intersites dans toutes les fenêtres (inclut les cookies de pistage),
> Contenu utilisé pour le pistage dans toutes les fenêtres,
> Mineurs de cryptomonnaies,
> Détecteurs d'empreinte numérique.

>>> vous pouvez naviguer dans une fenêtre privé qui ne conserve pas l'historique.

Installer des extensions

> **Ublock** : bloquer les publicités,
> **HTTPSEverywhere** : forcer le passage en httpS,
> **Decentraleyes** : se protéger du pistage lié aux diffuseurs de contenus CDN « gratuits », centralisés,
> **I don't care about cookies** : se débarrasser des alertes cookies,
> **Chameleon** : falsifier le profil de votre navigateur,
> (radical) **NoScript** : bloquer les scripts JavaScript, Java, Flash et autres.

La navigation incognito



TorProject.org

Changer de moteur de recherche

Duckduckgo

Changer de Cloud

Ne plus héberger ses données personnelles chez google ou microsoft
mais chez un tiers de confiance (https://www.chatons.org/)
ou chez soi.

Nextcloud

YUNO HOST

Utilisation du PC de quelqu'un d'autre

> Éviter les sites sur lesquels on saisit des données personnelles : webmail, réseaux sociaux, banque,etc...
> Vérifier que le navigateur est à jour.
> Ne pas mémoriser vos informations confidentielles
> Effacer vos traces de navigation & penser à fermer votre session
> Ne pas brancher de clef USB (virus), ne pas récupérer de documents.
> Idéalement ? Un navigateur en mode portable, depuis une clef USB
Encore mieux : rebooter sur un live-usb/cd

Wi-Fi public ?

Ne pas avoir confiance. Utiliser sa propre machine.

Attention à la sécurisation :
> Au minimum : vérifier que vous êtes en connexion HTTPS
> Mieux, passer par TOR (ou un VPN).

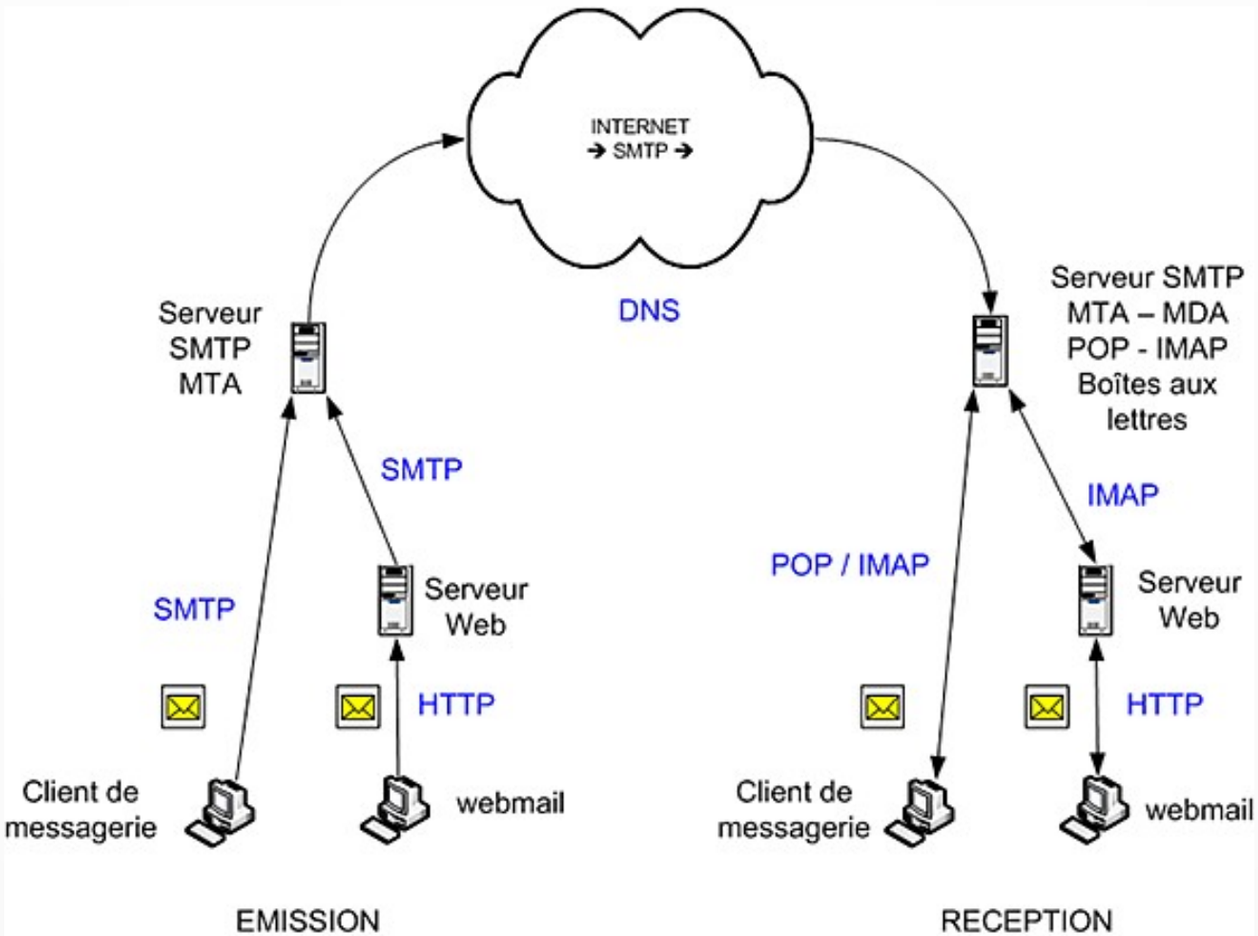
L’impact environnemental du numérique

> La **fabrication des objets numériques** (smartphones, pc,etc…) est **le principal facteur de pollution** environnemental du numérique.
« pour une puce électronique de 2 grammes, il faut 32 kg de matière première, soit 16 000 fois son poids ! » (https://www.greenit.fr/2020/05/26/500-fois-son-poids-en-matiere-premiere/)

> L’utilisation de services souvent surdimensionnés est aussi un facteur à interroger (google réplique nos mails dans plusieurs datacenters sur plusieurs continents).

> Les usages sont aussi à réfléchir.
« La vidéo en ligne génère en 2019 60 % des flux de données mondiaux. » et produit entre 50 et 300 millions de tonnes d’équivalent CO2 par an.
(https://fr.wikipedia.org/wiki/Vid%C3%A9o_%C3%A0_la_demande#Impact_environnemental)

Hygiène numérique & mail



- **Le webmail** : Interface sous forme de site web permettant de consulter ses emails via un navigateur web. Le webmail est mis à disposition par votre fournisseur de mail.
  Vous consultez vos mails « en ligne » sur le serveur de votre fournisseur sans les télécharger localement sur votre ordinateur.
- **Le client mail** : ou client de messagerie est un logiciel installé sur votre ordinateur qui sert à consulter et gérer ses emails (Thunderbird par exemple).Le client mail télécharge vos courriels sur votre ordinateur.
  Il permet de sauvegarder et d'archiver vos emails même si vous n'avez plus accès à votre compte mail.

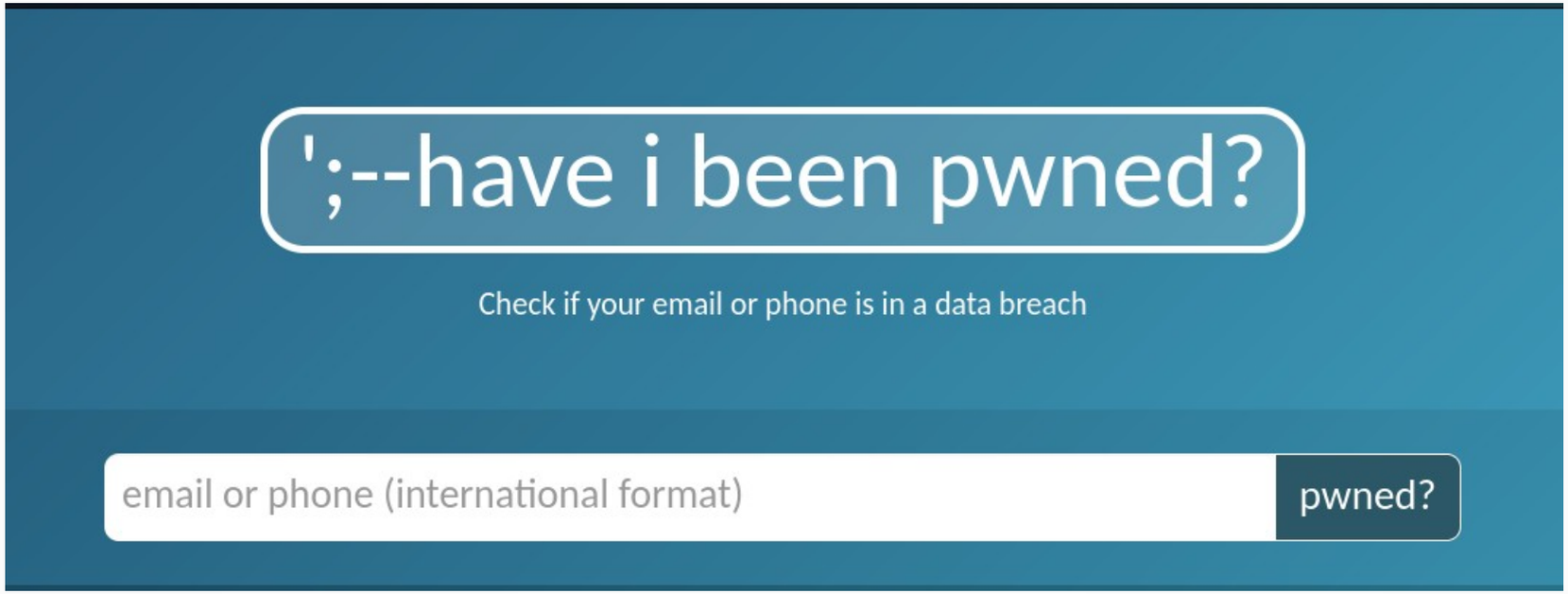
Les fournisseurs de mail

- Orange, free, sfr, etc.
- Gmail, hotmail, icloud, etc
- Protonmail
- Riseup
- Ilico.org (association corrézienne)

TOUS LES FOURNISSEURS SONT DES TIERS !

Mon mail a t'il fuité ?

https://haveibeenpwned.com/



Quelques dangers

- **Spam** (https://fr.wikipedia.org/wiki/Spam) : courrier indésirable ou pourriel
- **Phishing** (https://fr.wikipedia.org/wiki/Phishing) : technique utilisée par des fraudeurs pour obtenir des renseignements personnels
- **Spoofing** (https://blog.provectio.fr/email-spoofing-lutter-contre-le-spam-par-usurpation-didentite/) : technique d'usurpation d'identité qui consiste à envoyer des messages en se faisant passer pour quelqu'un d'autre.

Les pièces jointes

- En réception : bien regarder l'extension du fichier, en cas de doute : l'analyser (ou la supprimer).
- En envoi : taille limite des fichiers pour envoi dans le mail (https://epifil.com/blog/limites-des-boites-mail-et-webmail), pour envoyer plus gros utiliser un service en ligne (https://l.walrus.tf/ , https://drop.sans-nuage.fr/).
- Lors d'envoi à des destinataires multiples, une bonne pratique est d'utiliser un service en ligne pour stocker une fois votre fichier puis coller le lien fourni dans votre mail.
- Si vous possédez un « nuage », une extension du logiciel thunderbird permet d'automatiser la mise en ligne de votre pièce jointe et l'insertion du lien dans votre mail.

MERCI DE VOTRE ATTENTION !!!

Association MedicationTime

https://medicationtime.org/
contact@medicationtime.org

Supports des ateliers disponibles sur https://trashuniverse.org/

Atelier soutenu par la