Se protéger des écoutes (dans le réseau) et intrusions (dans les ordinateurs)

- **Chiffrement** : interdire la lecture par modification du message en le rendant illisible (brouillage)
- **Mots de passe** : bloquer l'accès pour des raisons d'authentification

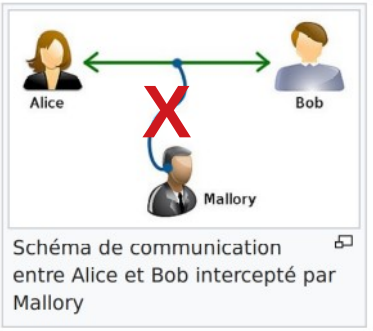


Schéma de communication entre Alice et Bob intercepté par Mallory

Quelques règles d'hygiène numérique
https://framatube.org/videos/watch/a2db0f2d-1d35-4d53-acb1-85fb0a8ae906

Protection des accès par mot de passe

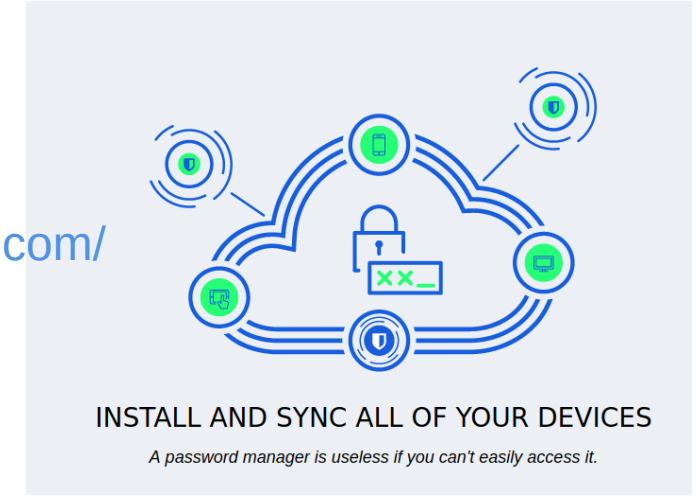
- À ne pas confondre avec le chiffrement
- Pour s'assurer d'un accès légitime

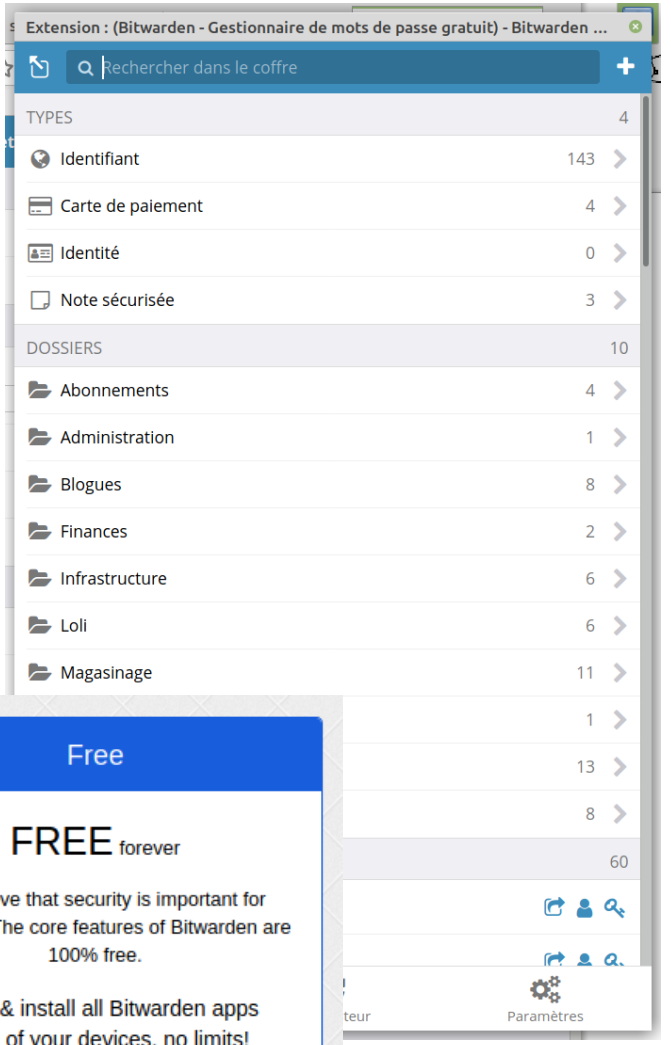
- But : s'assurer que l'accès est autorisé, il doivent être
  - difficiles à deviner
  - idéalement faciles à mémoriser
  - changés périodiquement
  - **utilisés que pour un seul usage**
  - gardés secret
  - *pour les infos de récupération*
    - *mentir*
    - mais s'en rappeler

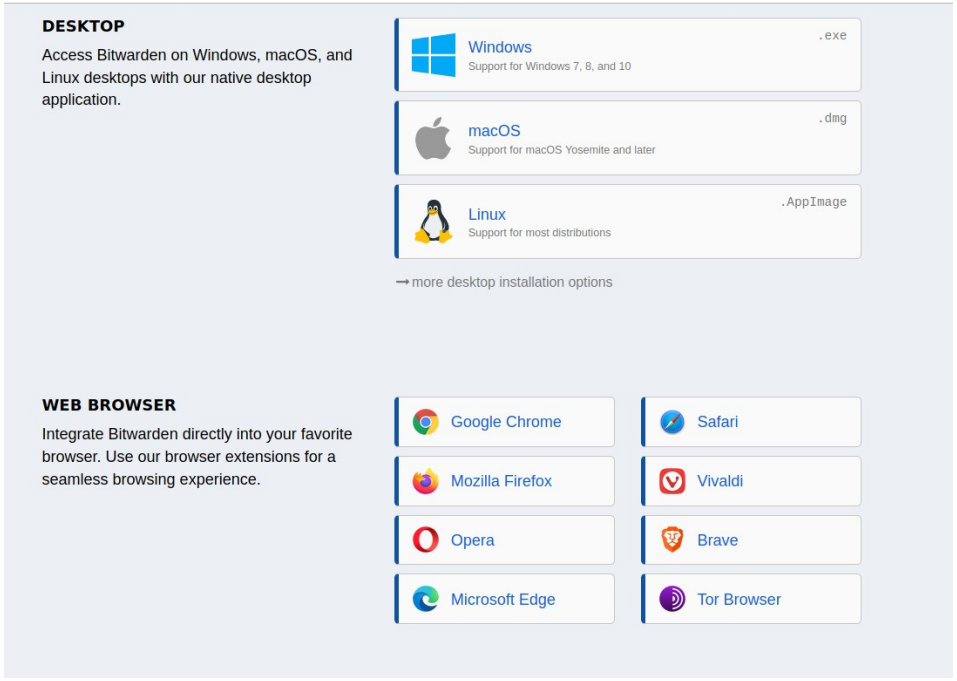
Une idée, la passe-phrase : 3 ou 4 mots du dictionnaire choisis au hasard

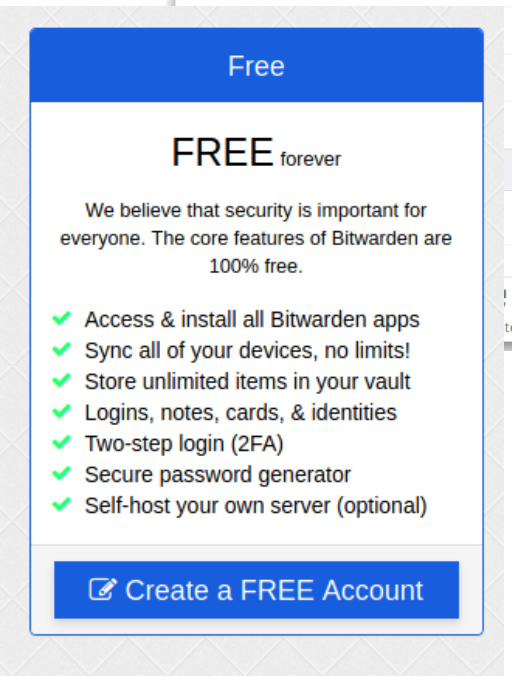
Bitwarden

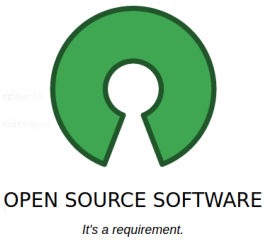
https://bitwarden.com/



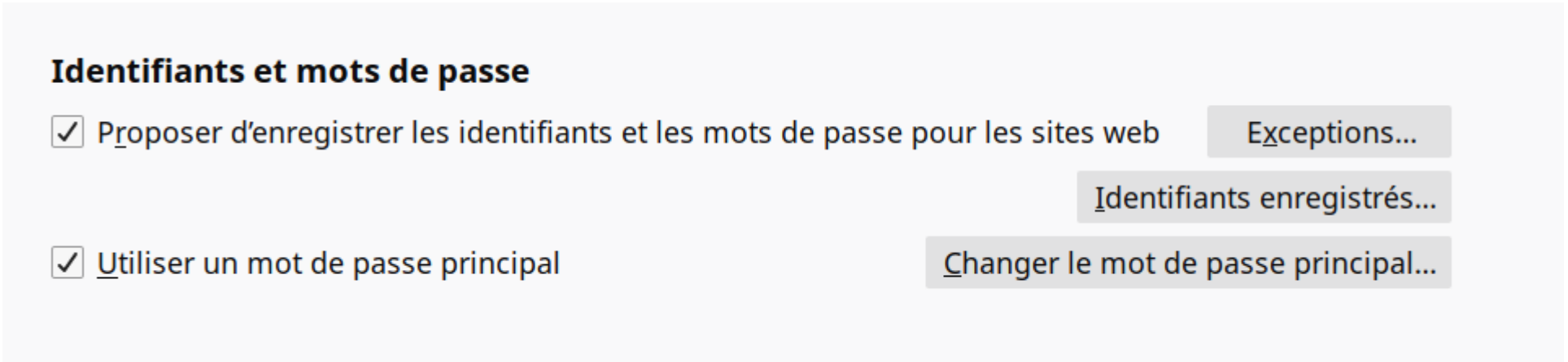


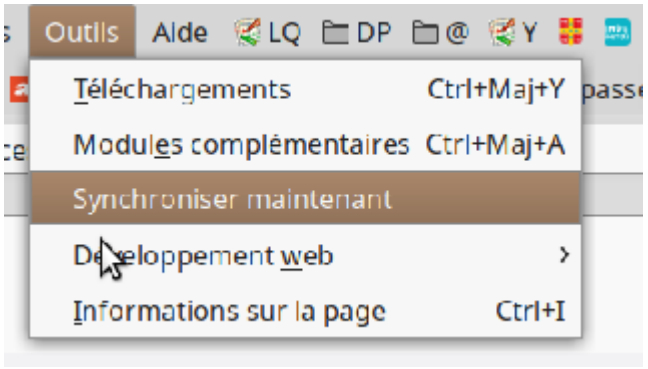






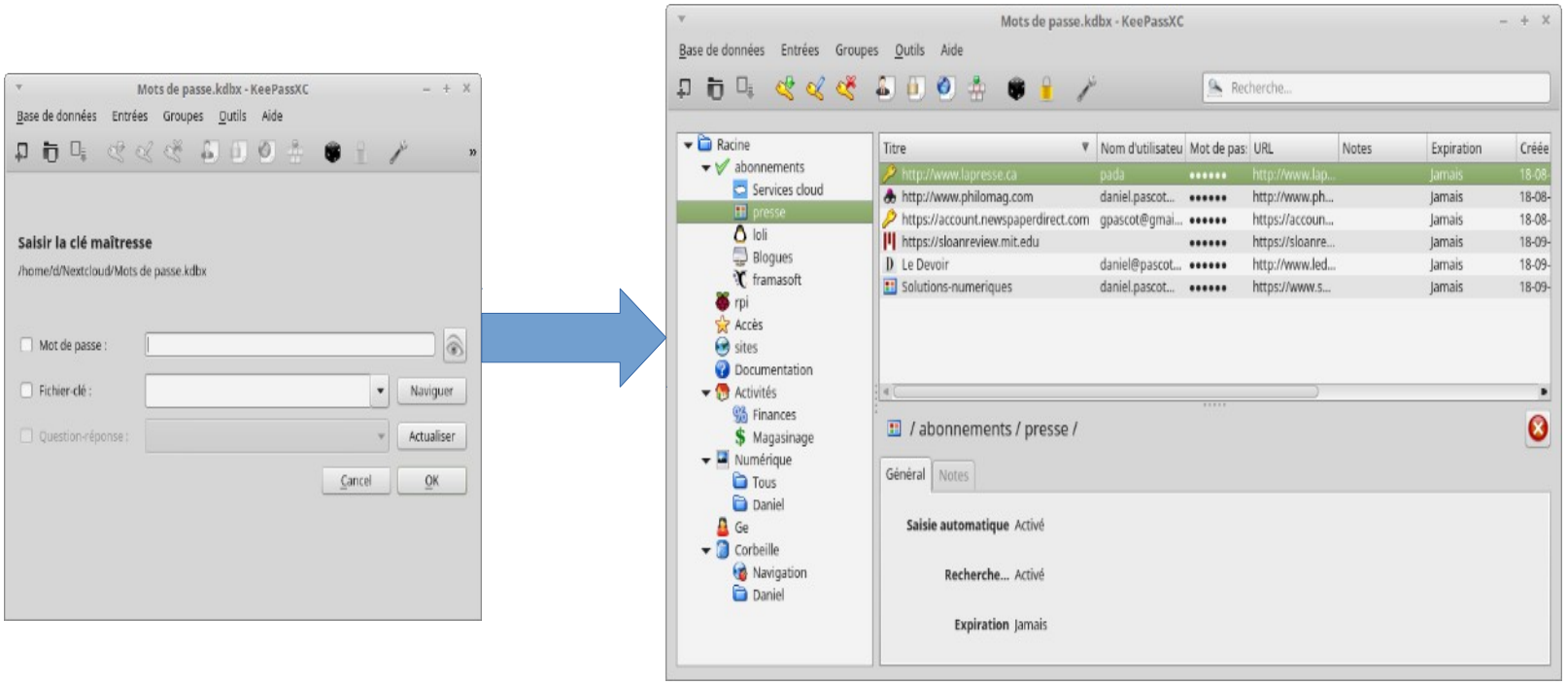
Il y en a aussi un incorporé dans les préférences de Firefox





Coffre fort de bons mots de passe

Une solution un logiciel sécurisé pour les conserver, par exemple keepassXC (c'est un logiciel libre multi plateforme de qualité avec une bonne communauté de support)



On peut la transporter sur une clé USB, le stocker dans le nuage car elle est bien protégée

Ne pas confondre chiffrement et codage

- Le codage transforme simplement : code morse ou compression
- Le chiffrement vise à interdire la lecture non autorisée
  - Symétrique : la même clé chiffre et déchiffre
  - Asymétrique une clé chiffre, une autre déchiffre

Le chiffrement est réalisé par un programme - de préférence libre- (qui met en œuvre un algorithme) contrôlé par une clé en entrée (parfois aussi appelé mot de passe) pour chiffrer et déchiffrer
La clé ne dois pas être diffusée ni perdue, c'est comme un mot de passe

Protection par chiffrement symétrique

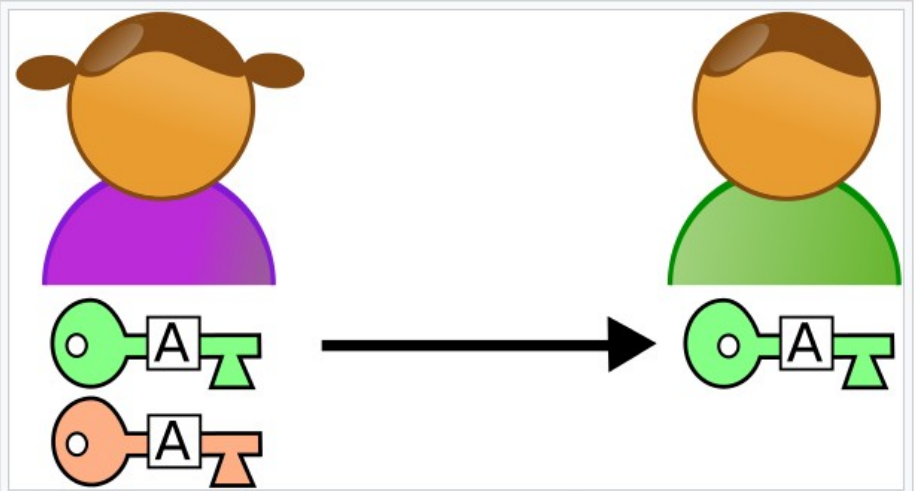
- Le contenu de son ordinateur ou téléphone
- Des dossiers ou documents (fichiers) sur son ordinateur
- Des dossiers ou documents avant d'envoi dans des dépôts externes

C'est la même personne qui chiffre et déchiffre

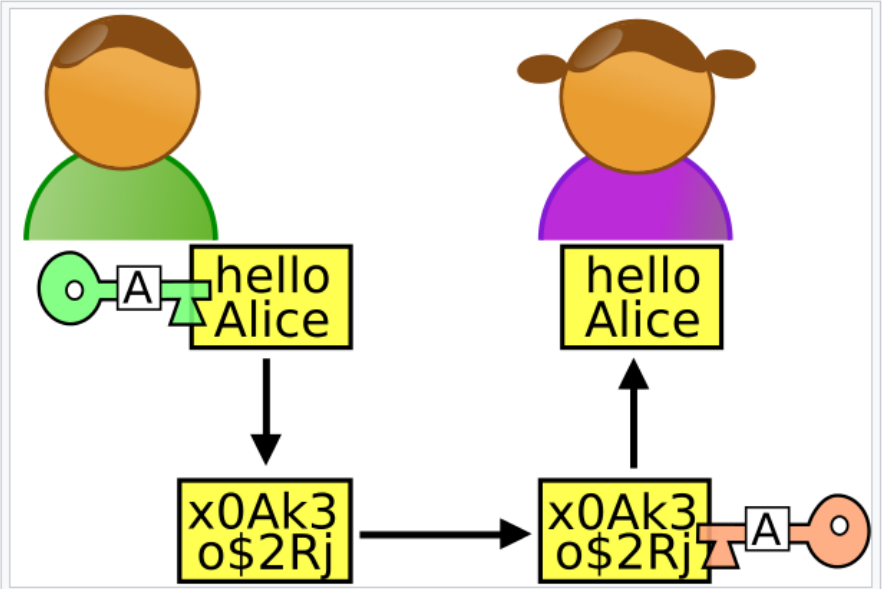
Utile quand on veut se protéger des situations telles que des intrusions (lectures non désirées accidentelles ou pas) ou la perte d'un matériel

Chiffrement par clés asymétriques : pour les communications

Ici Bob veut envoyer un message chiffré à Alice



1re étape : Alice génère deux clefs. La clef publique (verte) qu'elle envoie à Bob et la clef privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.



2e et 3e étapes : Bob chiffre le message avec la clef publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clef privée.

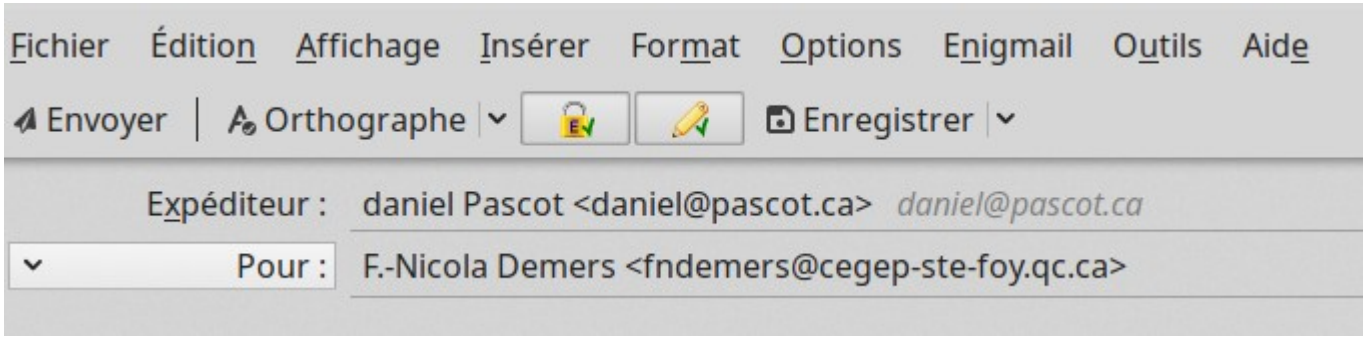
https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique

https://linuq.org/logiciels/gnupg

La clé de déchiffrement ne doit pas circuler

Protéger les contenus des communications

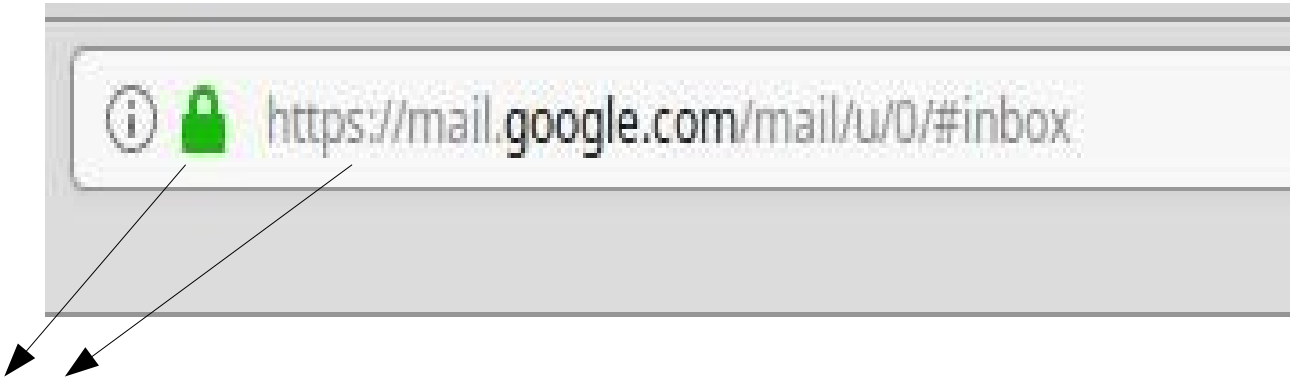
- Il faut chiffrer avant d'envoyer et déchiffrer après la réception, donc privilégier le chiffrement asymétriquet
- Dans le logiciel de courriel (contraignant car il faut échanger et gérer les clés)



- Si un assez grand pourcentage des communications sont chiffrées cela rend l'espionnage de masse inefficace et inutile

Attention

Ce n’est pas parce que la connexion est protégée contre les écoutes en ligne que celui avec lequel on communique ne nous espionne pas et que l’on peut vous identifier

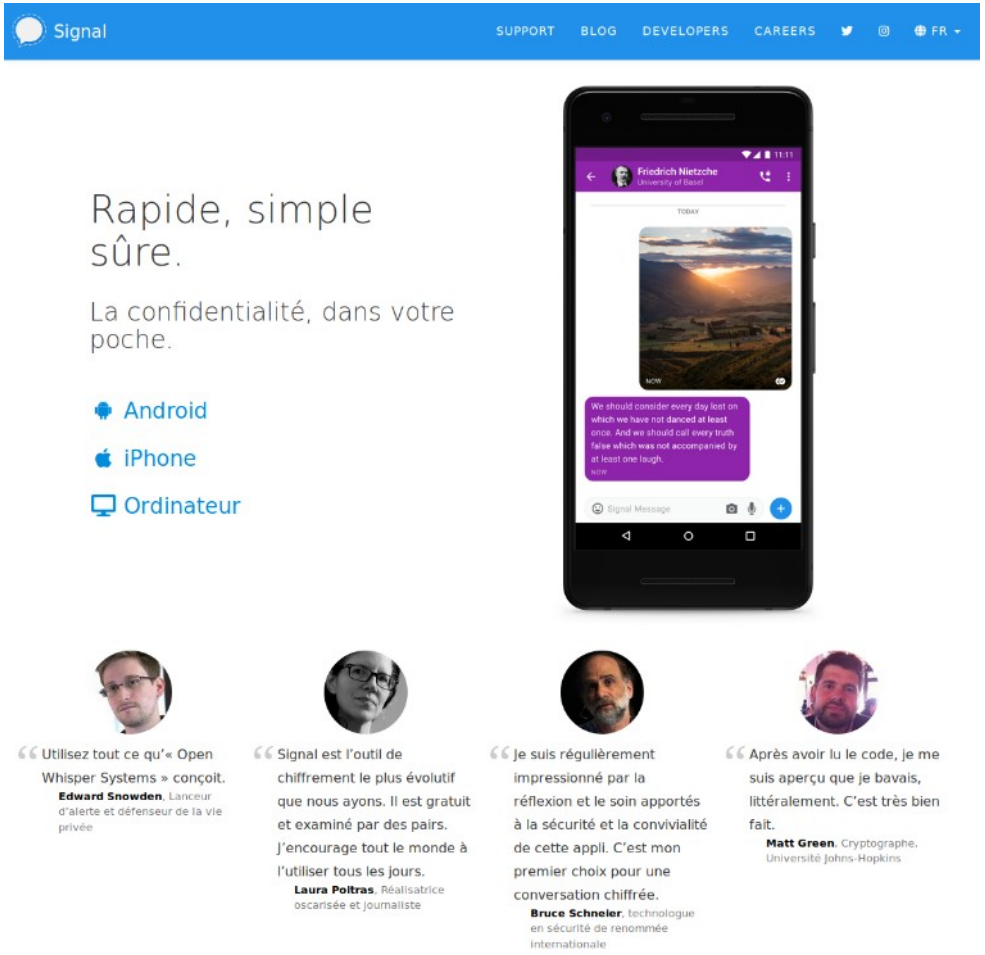


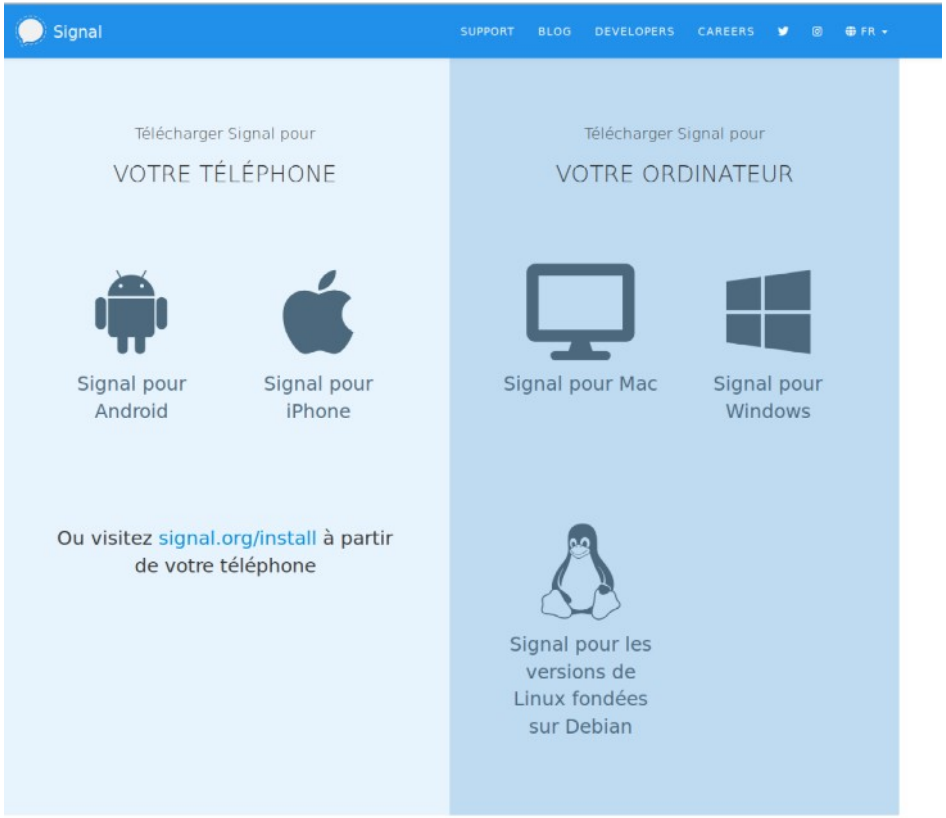
Indique que le message est chiffré pendant le transfert (et seulement le transfert)

Confidentialité : chiffrer les connexions

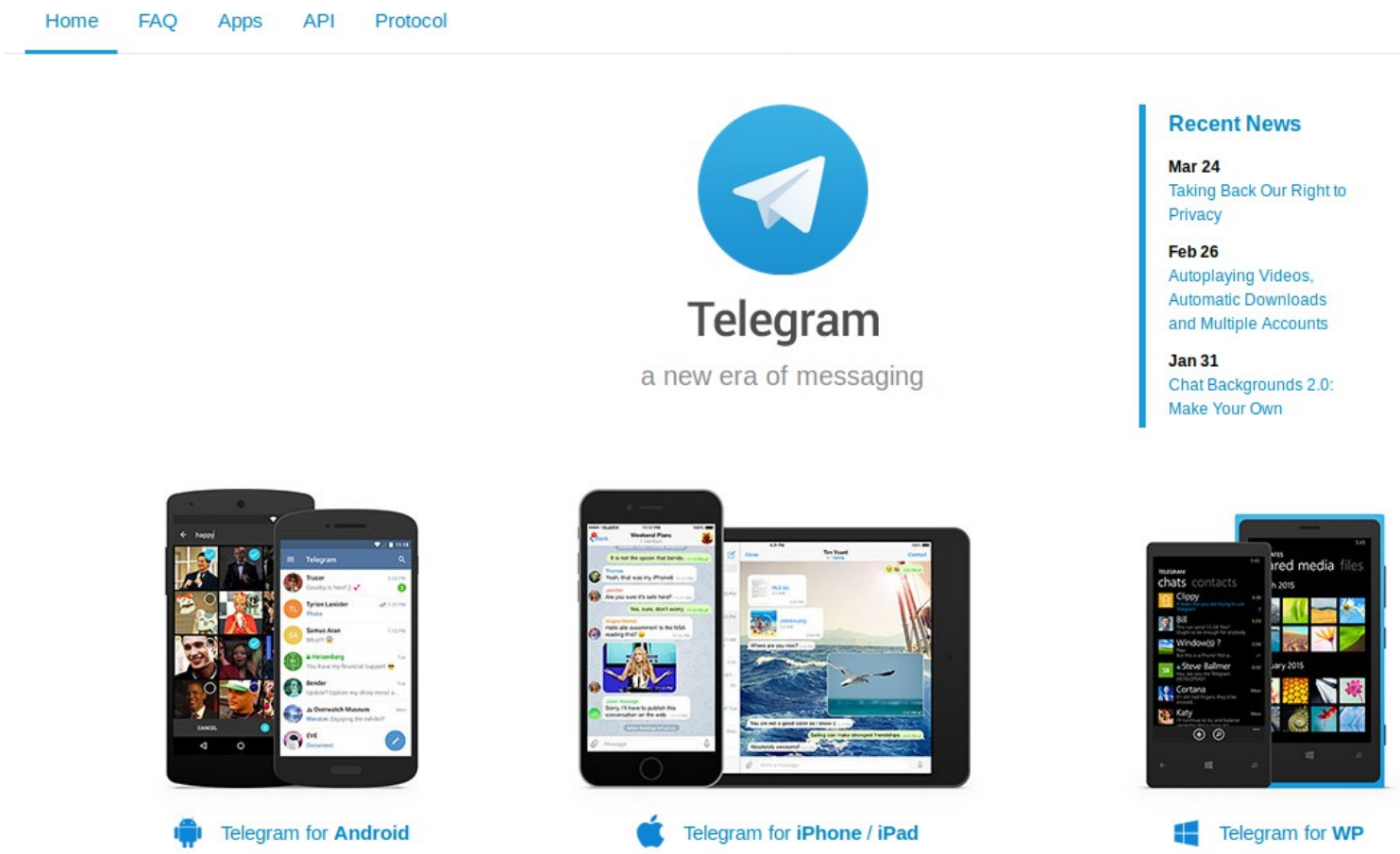
Savoir-faire LINUX

FREE SOFTWARE FOUNDATION
www.fsf.org

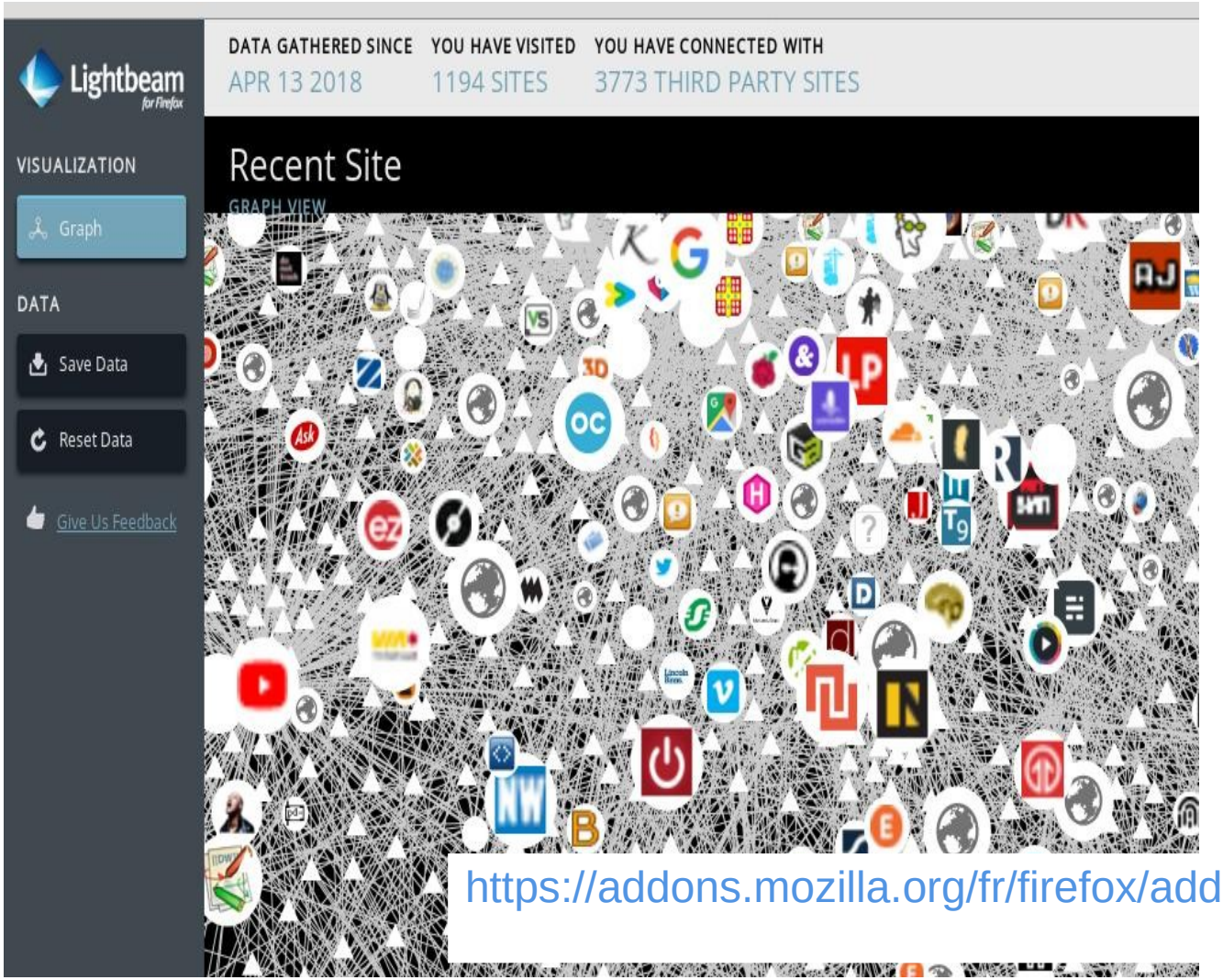




https://www.signal.org/


Home
FAQ
Apps
API
Protocol
Telegram
a new era of messaging
Recent News
Mar 24
Taking Back Our Right to Privacy
Feb 26
Autoplaying Videos, Automatic Downloads and Multiple Accounts
Jan 31
Chat Backgrounds 2.0: Make Your Own
Telegram for Android
Telegram for iPhone / iPad
Telegram for WP
A native app for every platform
https://telegram.org/

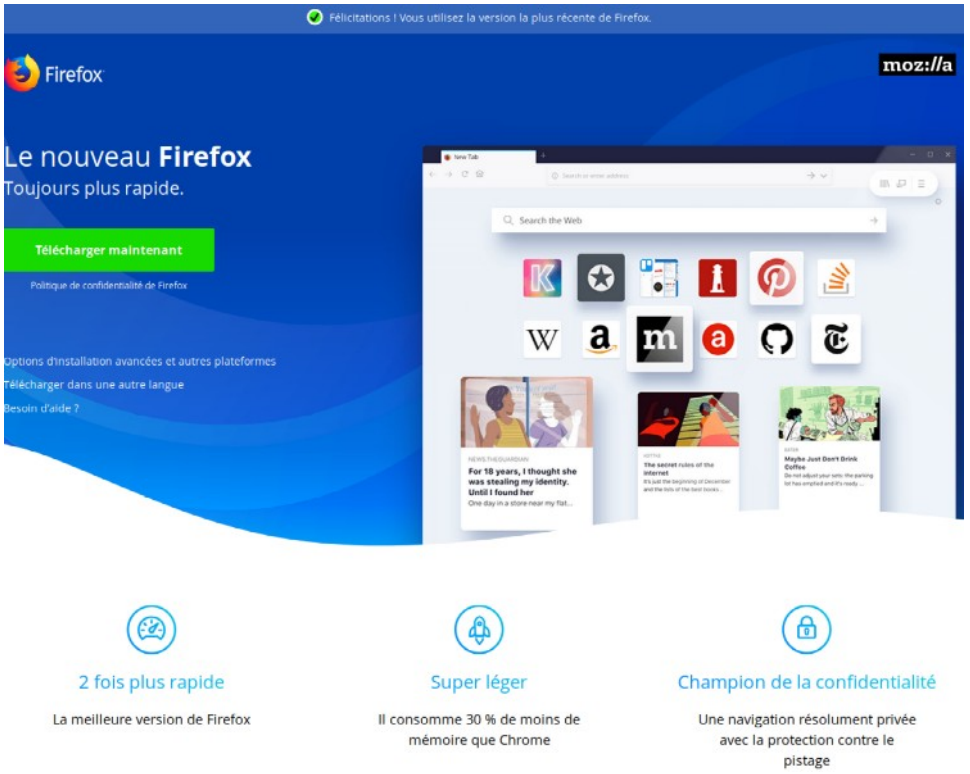
Un aperçu de l’espionnage généralisé à neutraliser : il se fait au niveau des applications



Lightbeam est une extension dans firefox

https://addons.mozilla.org/fr/firefox/addon/lightbeam/

Contrôler nos traces : choix du fureteur



Attention : toujours télécharger les logiciels libres depuis un site de confiance : normalement le site de la communauté qui le développe et l'entretient

Ne pas oublier les mises à jour

Un principe : il faut contrôler ce qui sort de votre ordinateur par le fureteur

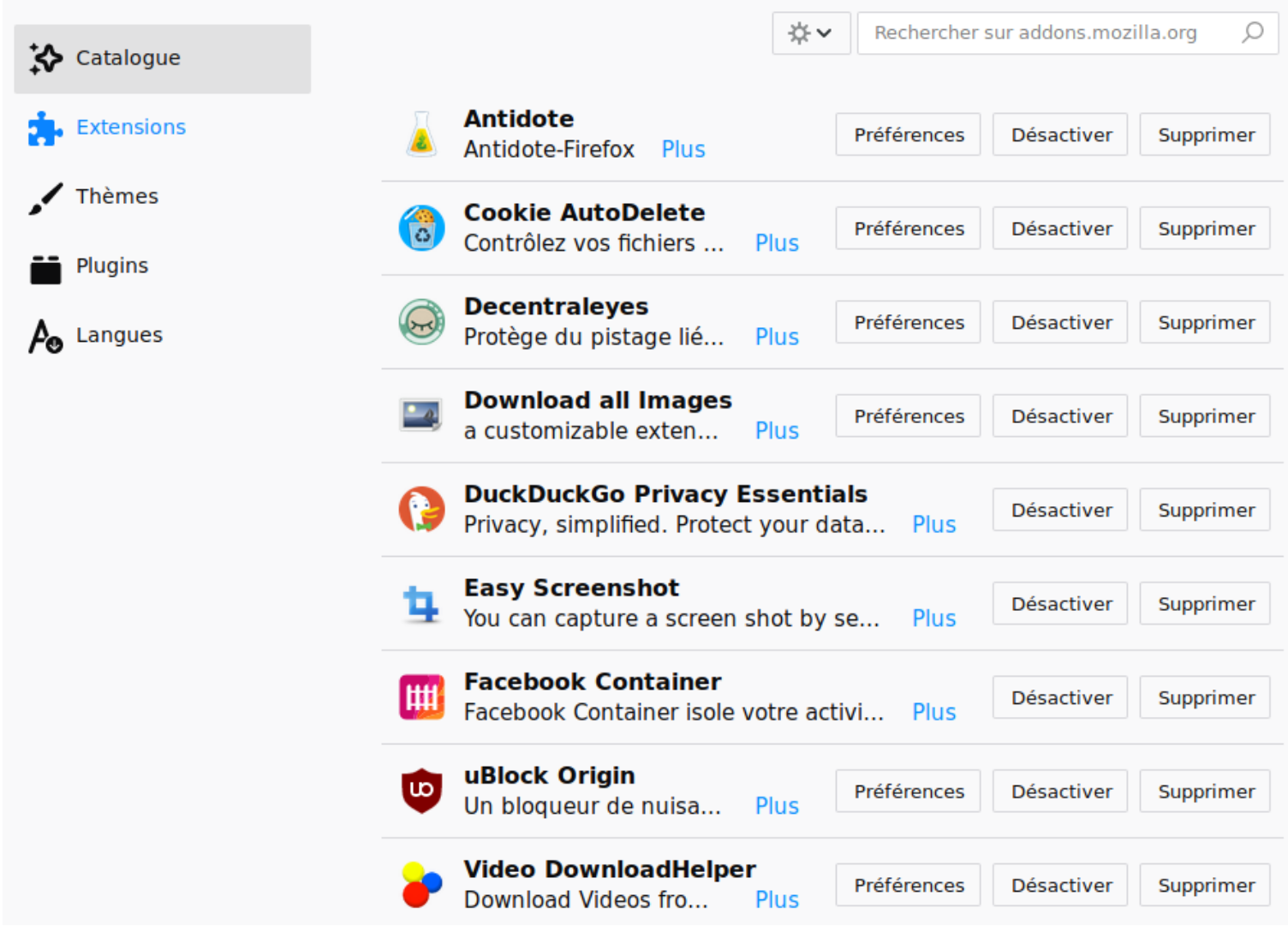
https://www.mozilla.org/fr/firefox/new/?redirect_source=firefox-com

Pour configurer et utiliser Firefox voir la présentation de François Pelletier (Linuq)
https://git.francoispelletier.org/francois/linuq-semaine-numeriqc-proteger-fureteur/src/branch/master/presentation.md

Ce qui vous menace ce n’est pas ce qui entre mais ce qui sort de votre ordinateur, tablette, téléphone

Bien sûr si ça sort c’est que quelque chose l’a fait sortir

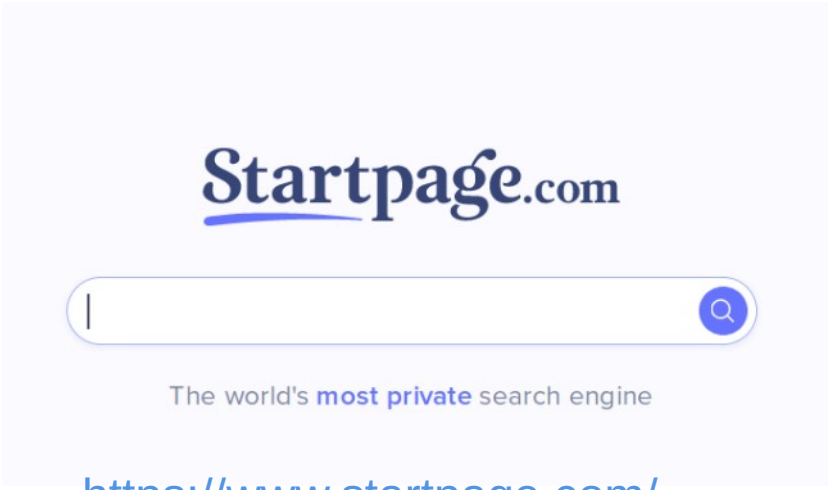
Un choix d’extensions (François)



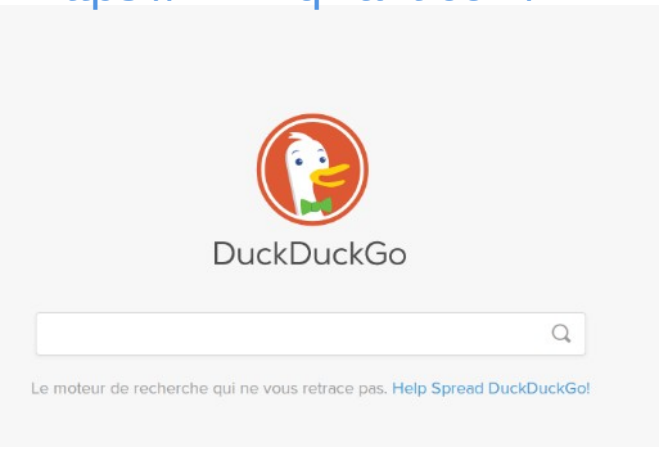
https://git.francoispelletier.org/francois/linuq-semaine-numeriqc-proteger-fureteur/src/branch/master/presentation.md

Adoptez un moteur de recherche qui ne vous espionne pas

https://www.qwant.com/



https://www.startpage.com/



https://duckduckgo.com/

Brouillez les pistes avec un vpn : cacher des métadonnées

Fuyez les services gratuits

Sujet traité dans un atelier Linuq

https://linuq.org/vie-privee/proteger_navigateur

Soyez prudents et vigilants, adoptez de bonnes pratiques

- N’utilisez que des connexions sécurisées
- Préférez les accès par fureteur : vous avez le maximum de contrôle en le paramétrant
- Attention aux applications dédiées :
  - Vous n’avez aucun contrôle sur les données qu’elles envoient
  - Renseignez-vous sur ce qu’elles communiquent
- Conseil : commencez par l’essentiel, maîtriser le avant de trop en faire sans le comprendre. En ce domaine trop devient vite comme pas assez