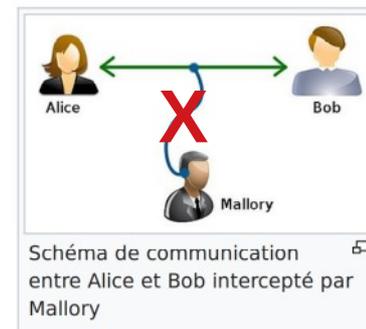


# Se protéger des écoutes (dans le réseau) et intrusions (dans les ordinateurs)

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



Quelques règles d'hygiène numérique

<https://framatube.org/videos/watch/a2db0f2d-1d35-4d53-acb1-85fb0a8ae906>

# Protection des accès par mot de passe



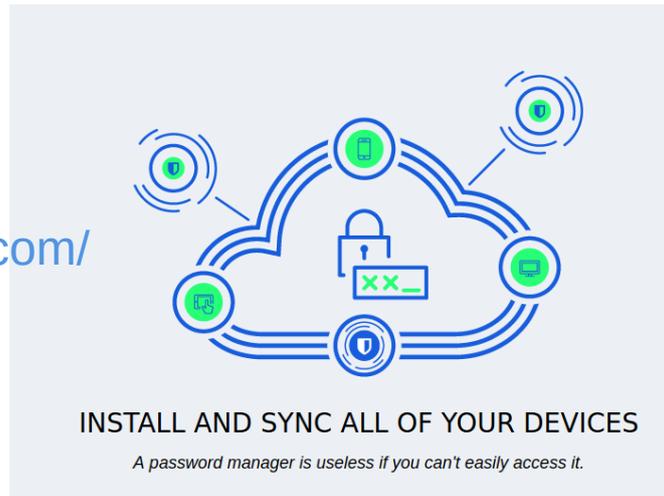
- But : s'assurer que l'accès est autorisé, il doivent être
  - difficiles à deviner
  - idéalement faciles à mémoriser
  - changés périodiquement
  - **utilisés que pour un seul usage**
  - gardés secret
  - *pour les infos de récupération*
    - *mentir*
    - mais s'en rappeler

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

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

# Bitwarden

<https://bitwarden.com/>



**DESKTOP**

Access Bitwarden on Windows, macOS, and Linux desktops with our native desktop application.

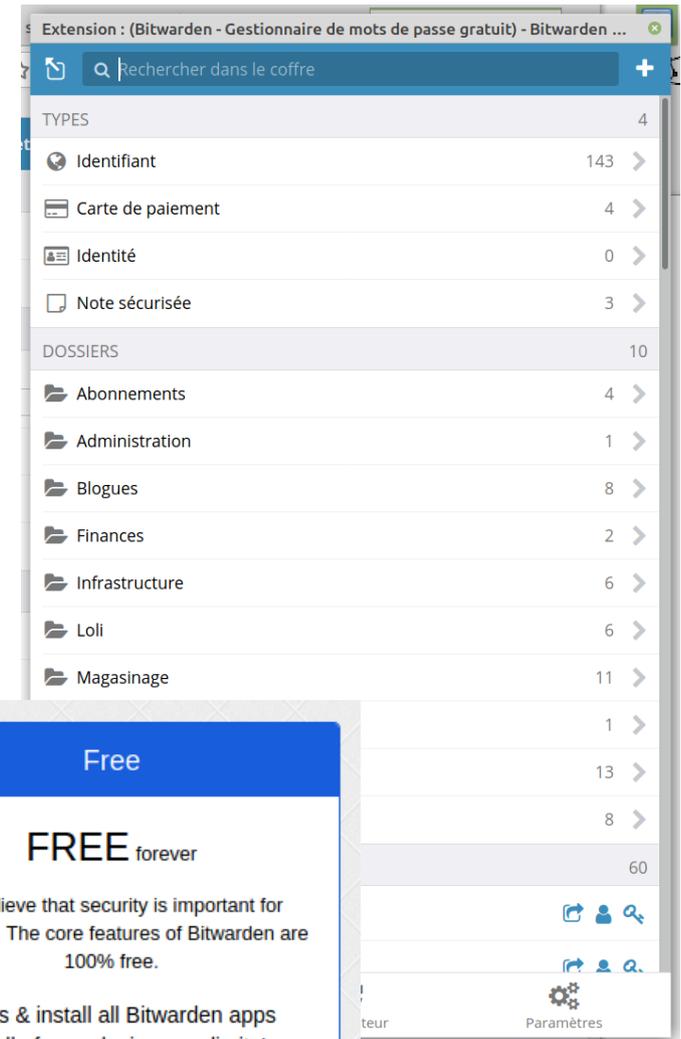
- Windows** (.exe)  
Support for Windows 7, 8, and 10
- macOS** (.dmg)  
Support for macOS Yosemite and later
- Linux** (.AppImage)  
Support for most distributions

→ more desktop installation options

**WEB BROWSER**

Integrate Bitwarden directly into your favorite browser. Use our browser extensions for a seamless browsing experience.

- Google Chrome
- Safari
- Mozilla Firefox
- Vivaldi
- Opera
- Brave
- Microsoft Edge
- Tor Browser



Free

**FREE** forever

We believe that security is important for everyone. The core features of Bitwarden are 100% free.

- ✓ Access & install all Bitwarden apps
- ✓ Sync all of your devices, no limits!
- ✓ Store unlimited items in your vault
- ✓ Logins, notes, cards, & identities
- ✓ Two-step login (2FA)
- ✓ Secure password generator
- ✓ Self-host your own server (optional)

Create a FREE Account



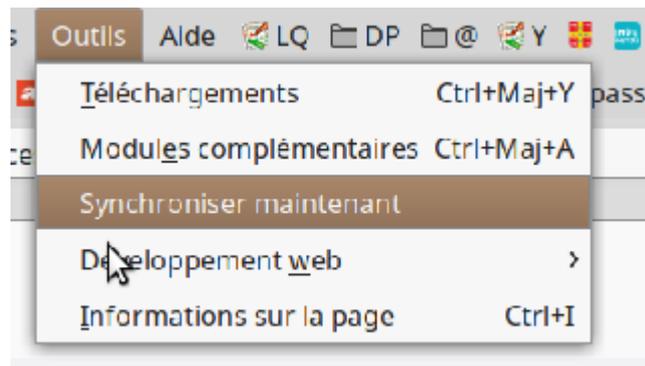
OPEN SOURCE SOFTWARE  
*It's a requirement.*



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

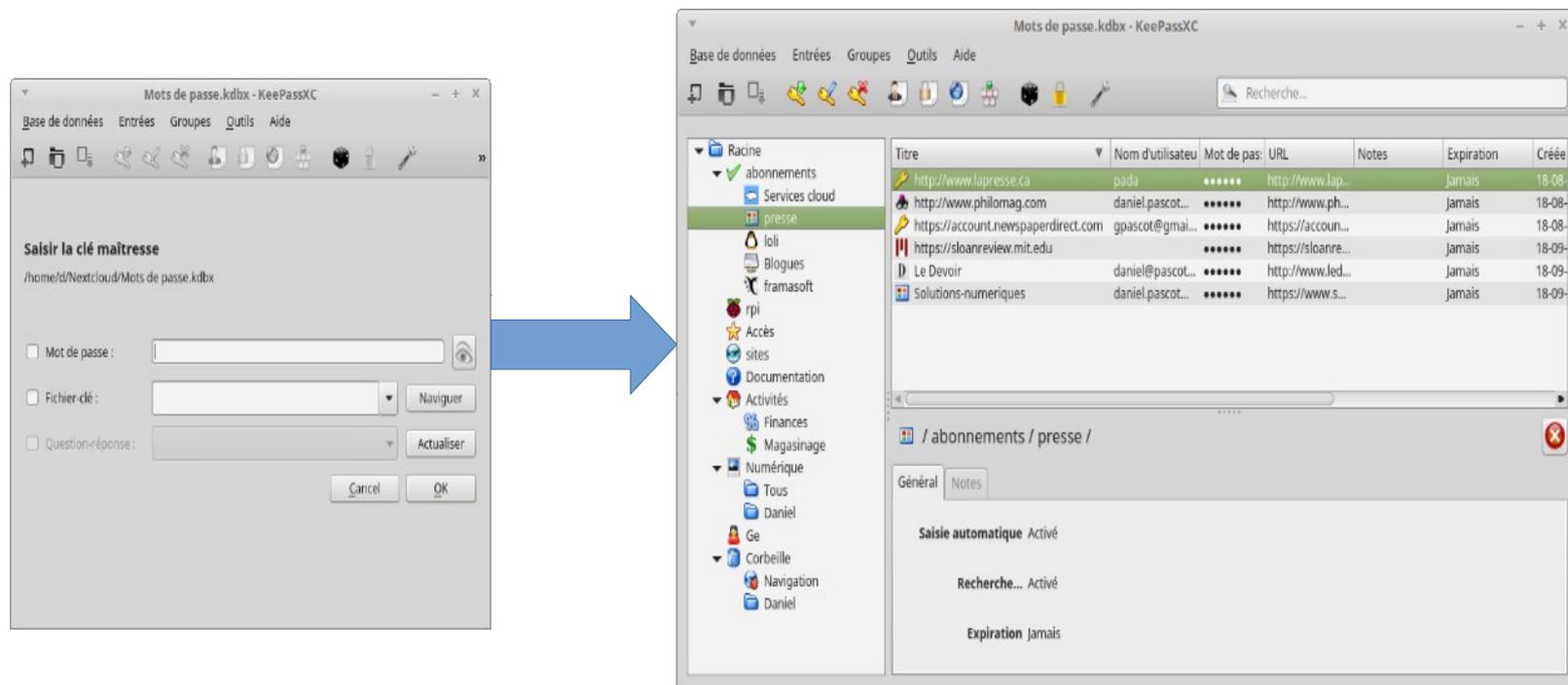
## Identifiants et mots de passe

- Proposer d'enregistrer les identifiants et les mots de passe pour les sites web [Exceptions...](#)
- Utiliser un mot de passe principal [Identifiants enregistrés...](#)
- [Changer le mot de passe principal...](#)



# 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 doit pas être diffusée ni perdue, c'est comme un mot de passe**

# Protection par chiffrement symétrique

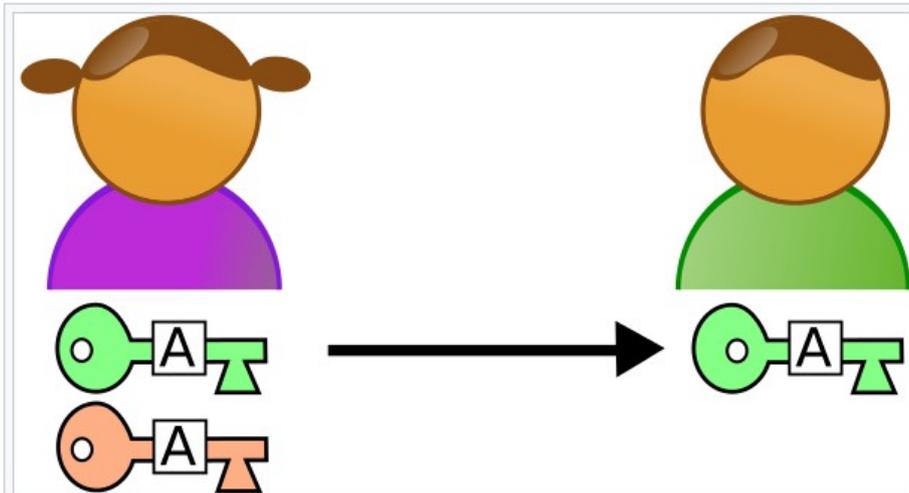
- Le contenu de son ordinateur ou téléphone
- Des dossiers ou documents (fichiers) sur son ordinateur
- Des dossiers ou documents avant d'envoi dans des dépôts externes

**C'est la même personne qui chiffre et déchiffre**

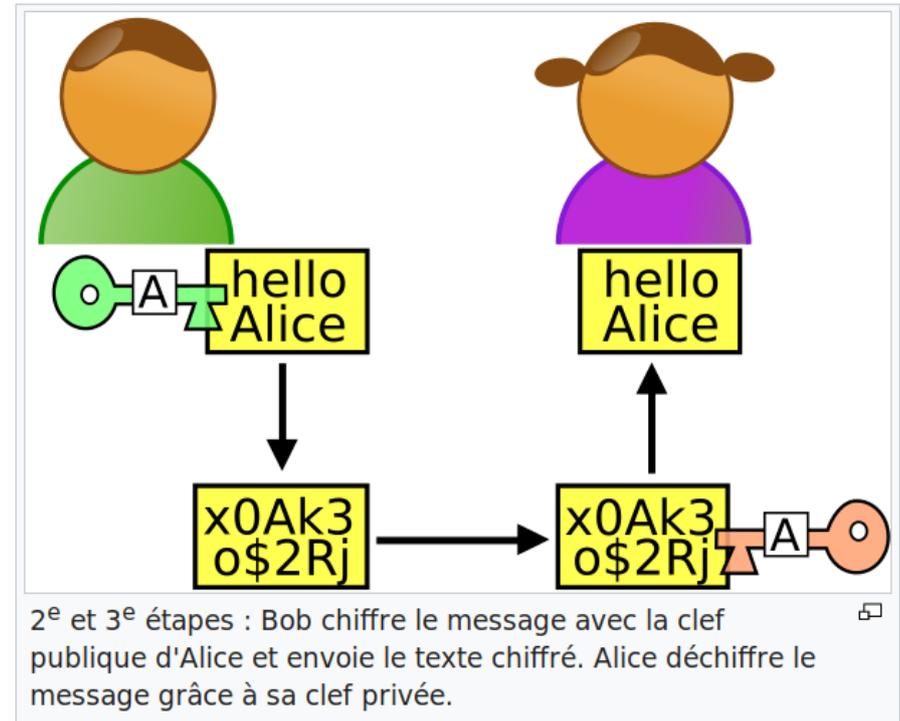
Utile quand on veut se protéger des situations telles que des intrusions (lectures non désirées accidentelles ou pas) ou la perte d'un matériel

# Chiffrement par clés asymétriques : pour les communications

Ici Bob veut envoyer un message chiffré à Alice



1<sup>re</sup> 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.



2<sup>e</sup> et 3<sup>e</sup> 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.

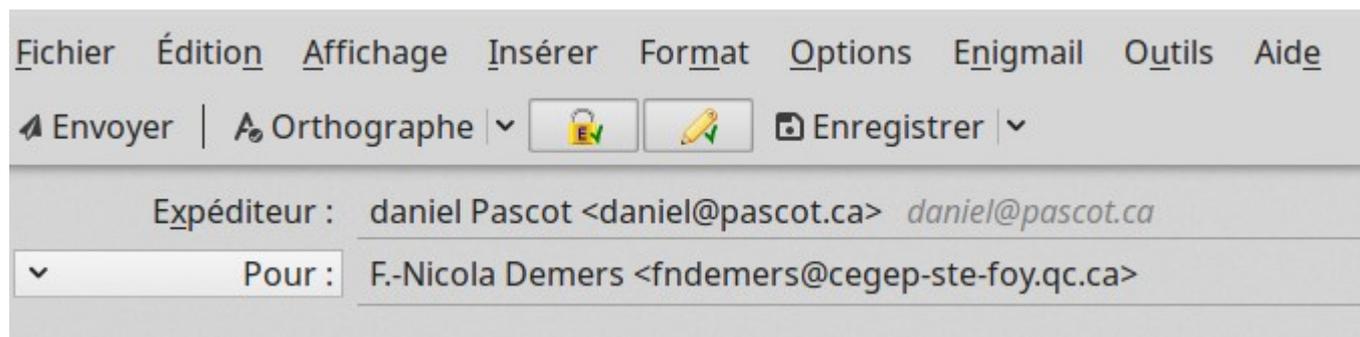
[https://fr.wikipedia.org/wiki/Cryptographie\\_asym%C3%A9trique](https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique)

<https://linuq.org/logiciels/gnupg>

La clé de  
déchiffrement  
ne doit pas  
circuler

# Protéger les contenus des communications

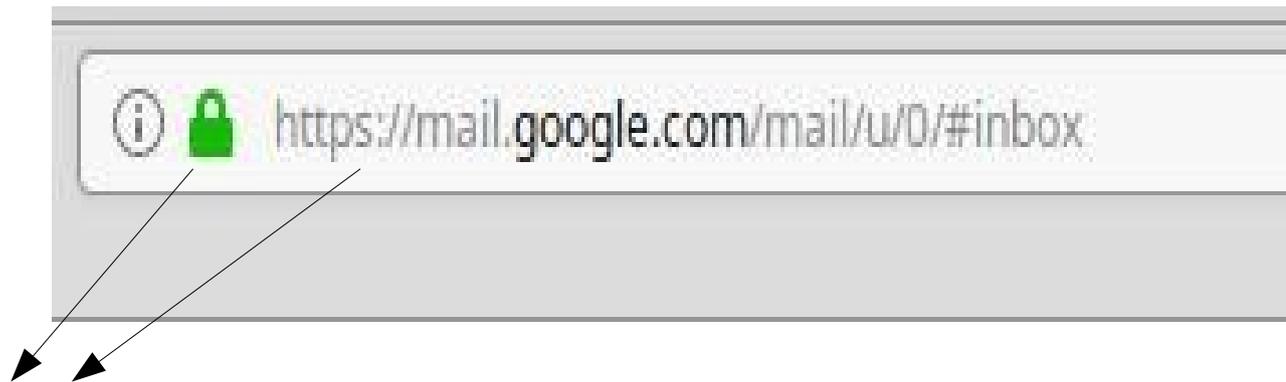
- Il faut chiffrer avant d'envoyer et déchiffrer après la réception, donc privilégier le chiffrement asymétrique
- Dans le logiciel de courriel (contraignant car il faut échanger et gérer les clés)



- 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

**Parlez. Regardez. Partagez.**

Télécharger Jami

Jami est une plateforme de communication universelle et libre, respectant les libertés et la vie privée des utilisateurs.

Jami est également disponible sur :

<https://jami.net/>



Rapide, simple  
sûre.

La confidentialité, dans votre poche.

-  Android
-  iPhone
-  Ordinateur



  
 « Utilisez tout ce qu' » Open  
 Whisper Systems » conçoit.  
**Edward Snowden**, Lanceur  
 d'alerte et défenseur de la vie  
 privée

  
 « Signal est l'outil de  
 chiffrement le plus évolutif  
 que nous ayons. Il est gratuit  
 et examiné par des pairs.  
 J'encourage tout le monde à  
 l'utiliser tous les jours.  
**Laura Poitras**, Réalisatrice  
 oscarisée et journaliste

  
 « Je suis régulièrement  
 impressionné par la  
 réflexion et le soin apportés  
 à la sécurité et la convivialité  
 de cette appli. C'est mon  
 premier choix pour une  
 conversation chiffrée.  
**Bruce Schneier**, technologue  
 en sécurité de renommée  
 internationale

  
 « Après avoir lu le code, je me  
 suis aperçu que je bavais,  
 littéralement. C'est très bien  
 fait.  
**Matt Green**, Cryptographe,  
 Université Johns-Hopkins

Signal SUPPORT BLOG DEVELOPERS CAREERS FR

Télécharger Signal pour  
VOTRE TÉLÉPHONE

  
 Signal pour  
Android

  
 Signal pour  
iPhone

Ou visitez [signal.org/install](https://signal.org/install) à partir  
de votre téléphone

Télécharger Signal pour  
VOTRE ORDINATEUR

  
 Signal pour Mac

  
 Signal pour  
Windows

  
 Signal pour les  
versions de  
Linux fondées  
sur Debian

<https://www.signal.org/>



# 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



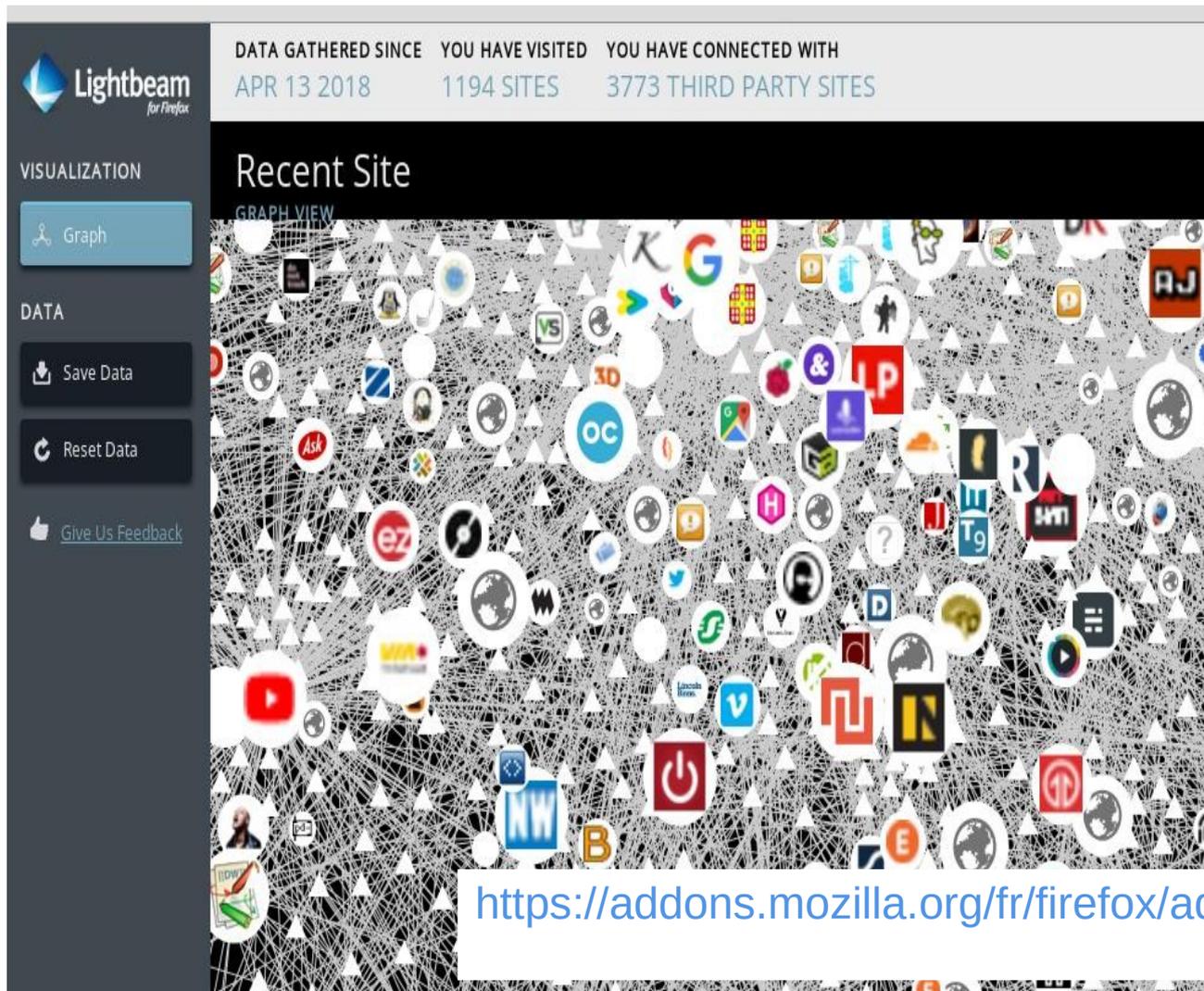
 Telegram for WP

A native app for every platform

<https://telegram.org/>



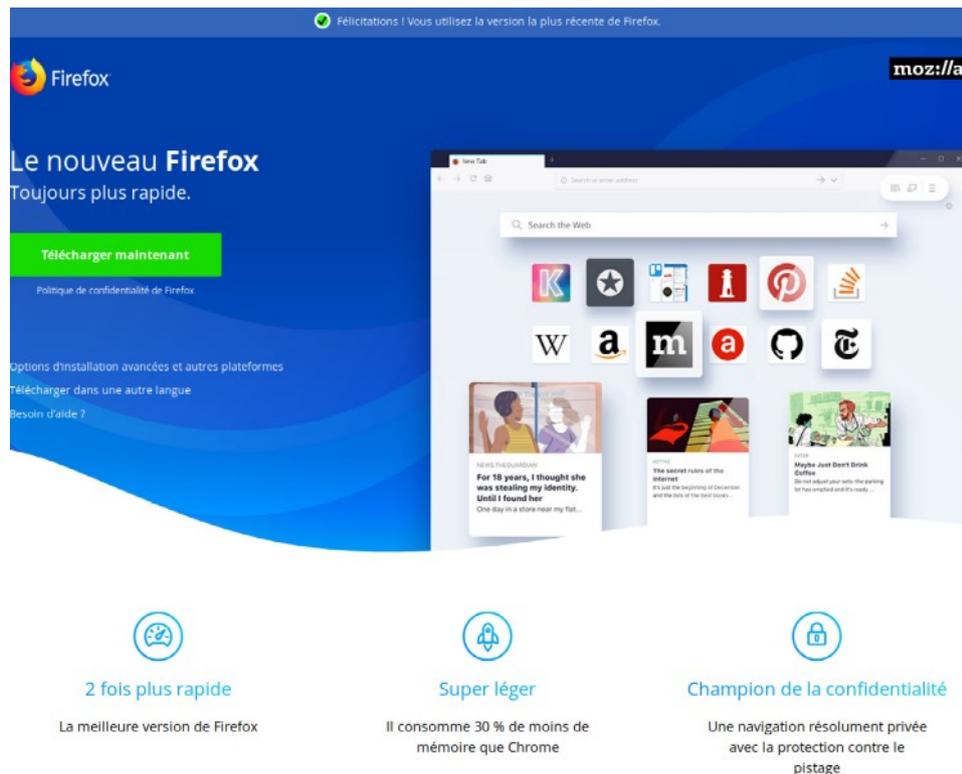
# Un aperçu de l'espionnage généralisé à neutraliser : il se fait au niveau des applications



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

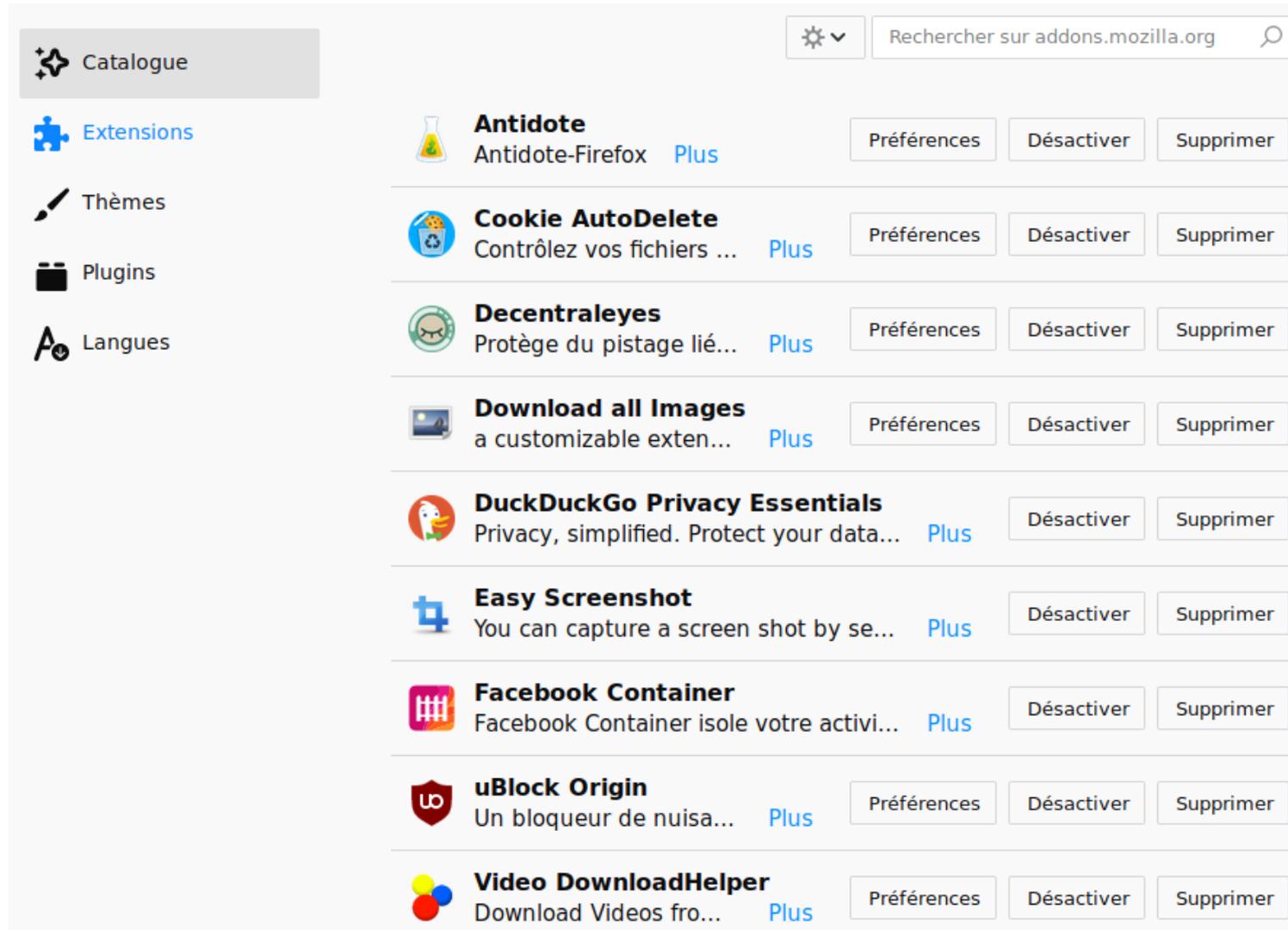
Pour configurer et utiliser Firefox voir la présentation de François Pelletier (Linuq)

<https://git.francoispelletier.org/francois/linuq-semaine-numeriqc-protoger-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 (Français)



The screenshot shows the Mozilla Add-ons website interface. On the left, there is a navigation menu with the following items: 'Catalogue' (selected), 'Extensions', 'Thèmes', 'Plug-ins', and 'Langues'. At the top right, there is a search bar with the text 'Rechercher sur addons.mozilla.org' and a search icon. The main content area displays a list of ten extensions, each with an icon, name, description, and three action buttons: 'Préférences', 'Désactiver', and 'Supprimer'. The extensions listed are:

- Antidote**: Antidote-Firefox Plus
- Cookie AutoDelete**: Contrôlez vos fichiers ... Plus
- Decentraleyes**: Protège du pistage lié... Plus
- Download all Images**: a customizable exten... Plus
- DuckDuckGo Privacy Essentials**: Privacy, simplified. Protect your data... Plus
- Easy Screenshot**: You can capture a screen shot by se... Plus
- Facebook Container**: Facebook Container isole votre activi... Plus
- uBlock Origin**: Un bloqueur de nuisa... Plus
- Video DownloadHelper**: Download Videos fro... Plus

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

# Adoptez un moteur de recherche qui ne vous espionne pas



Le moteur de recherche qui respecte votre vie privée.



<https://www.qwant.com/>

**Startpage.com**



The world's **most private** search engine

<https://www.startpage.com/>



DuckDuckGo



Le moteur de recherche qui ne vous retrace pas. Help Spread DuckDuckGo!

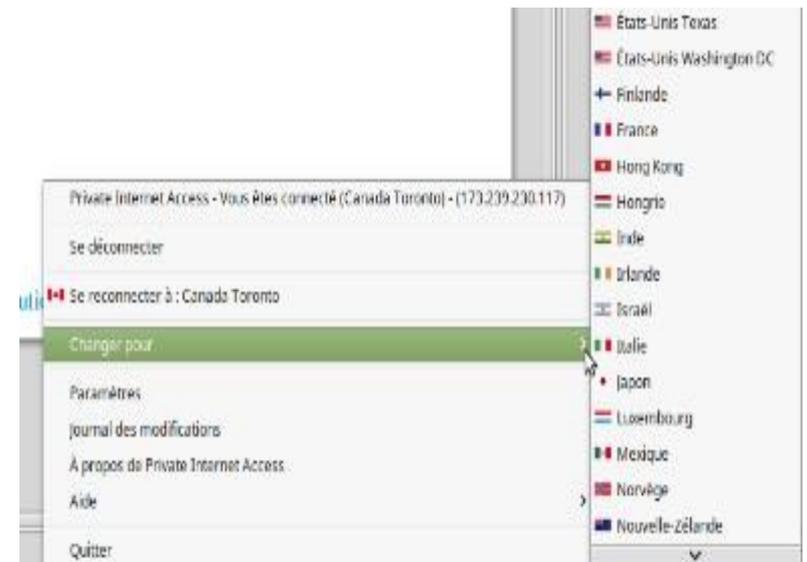
<https://duckduckgo.com/>

# 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](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 navigateur** : 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**