

Mieux protéger sa vie privée sur le net
CryptoParty Chiroux, 25/04

Table des matières

- Contexte
 - Prism ? Xkeyscore ?
 - Situation en Belgique
- Premiers réflexes
- Solutions logicielles
- Solutions internet
- Liens et contacts



Le contexte

Pourquoi se protéger ?

- L'actualité récente a démontré qu'il devient impératif de protéger ses données et outils informatiques, car notre vie privée est constamment mise à mal sur internet.
- Nous n'avons peut être rien à cacher, mais la vie privée est un droit inaliénable concédé par la charte des droits de l'homme.

Comment le scandale est arrivé

En juin 2013, un ancien consultant de la NSA, Edward Snowden, prit contact avec un journaliste du Guardian, avec en sa possession des milliers de documents sur les pratiques d'espionnage de l'agence, avec, entre autre les programmes PRISM et XKEYSCORE.

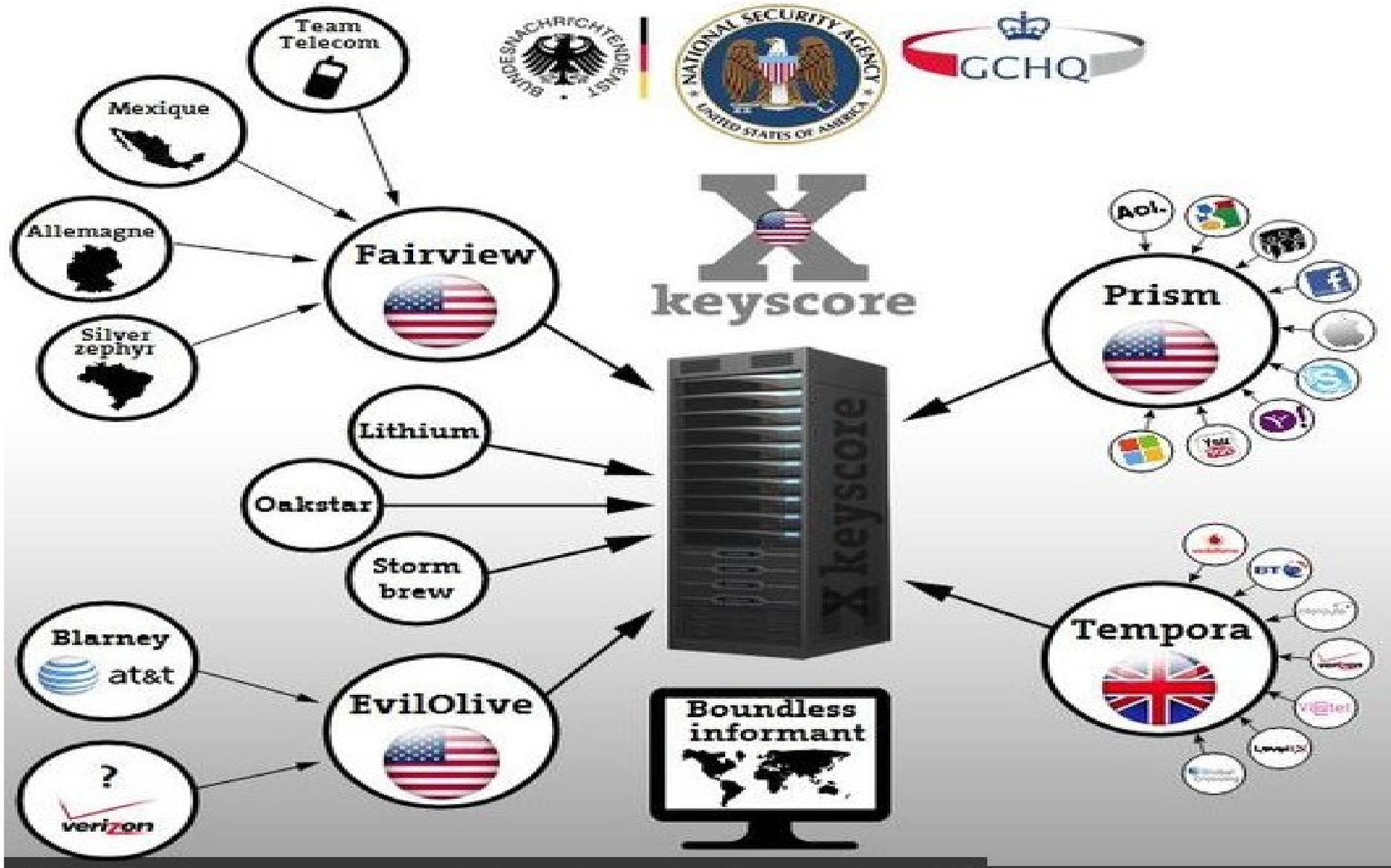
De semaines en semaines, les nouvelles révélations d'Edward démontrèrent que le monde entier était espionné par la NSA et GCHQ.



PRISM ? XKEYSCORE ?

- XKEYSCORE est une sorte de Méga moteur de recherche, une sorte de Google pour trouver des informations sur des individus et leurs activités.
- PRISM est une partie du programme XKEYSCORE qui donne un accès direct aux serveurs des acteurs majeurs du monde informatique.
- Nous pouvons apercevoir que Google, Microsoft, Apple, Yahoo, Facebook,... sont impliqués dans ce programme.

XKEYSCORE

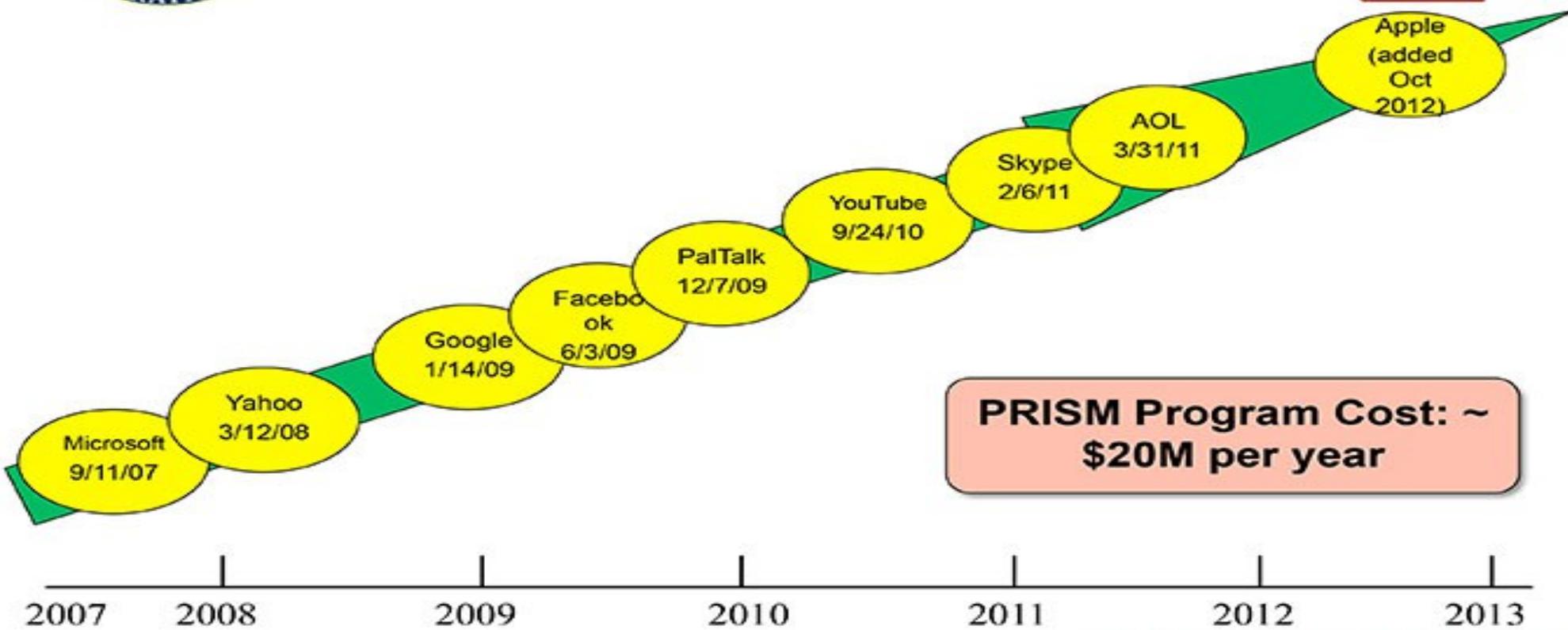


PRISM

TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ \$20M per year

TOP SECRET//SI//ORCON//NOFORN

Situation en belgique

- Depuis septembre dernier les FAI belges doivent enregistrer toute l'activité de leurs clients (suivant les directives européennes 2006/24/CE et 2002/58/CE)
- Ils doivent conserver toutes ces données pendant une année
- Présence d'un Firewall qui filtre le contenu d'internet en Belgique
- La N-VA, via le CPAS d'Anvers, fait espionner tous les allocataires sociaux anversoises sur internet

Premiers réflexes

Les mots de passe

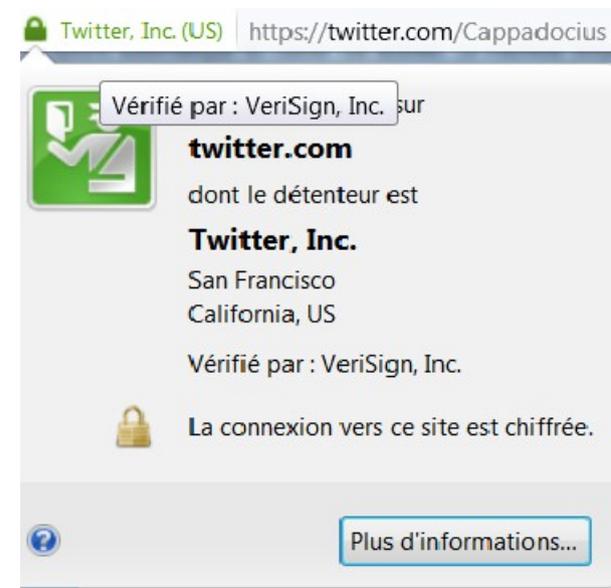
- Faire un bon mot de passe est le premier réflexe élémentaire à avoir, et pourtant c'est l'un des points forts négligé par la majorité des internautes.
- Toujours éviter noms, dates et éléments personnels.
- Toujours faire un mot de passe complexe, et si possible long, avec des lettres minuscules et majuscules, chiffres et caractères spéciaux :

J3-m@Ng3_Un3!P01r3

Https

Https est la version sécurisée du protocole http (hyper text transfert protocol), qui est utilisé pour surfer sur internet. Il permet de :

- Vérifier chez qui on est (petit cadenas vert).
- Sécuriser la visite d'un site internet, en utilisant une connexion chiffrée.

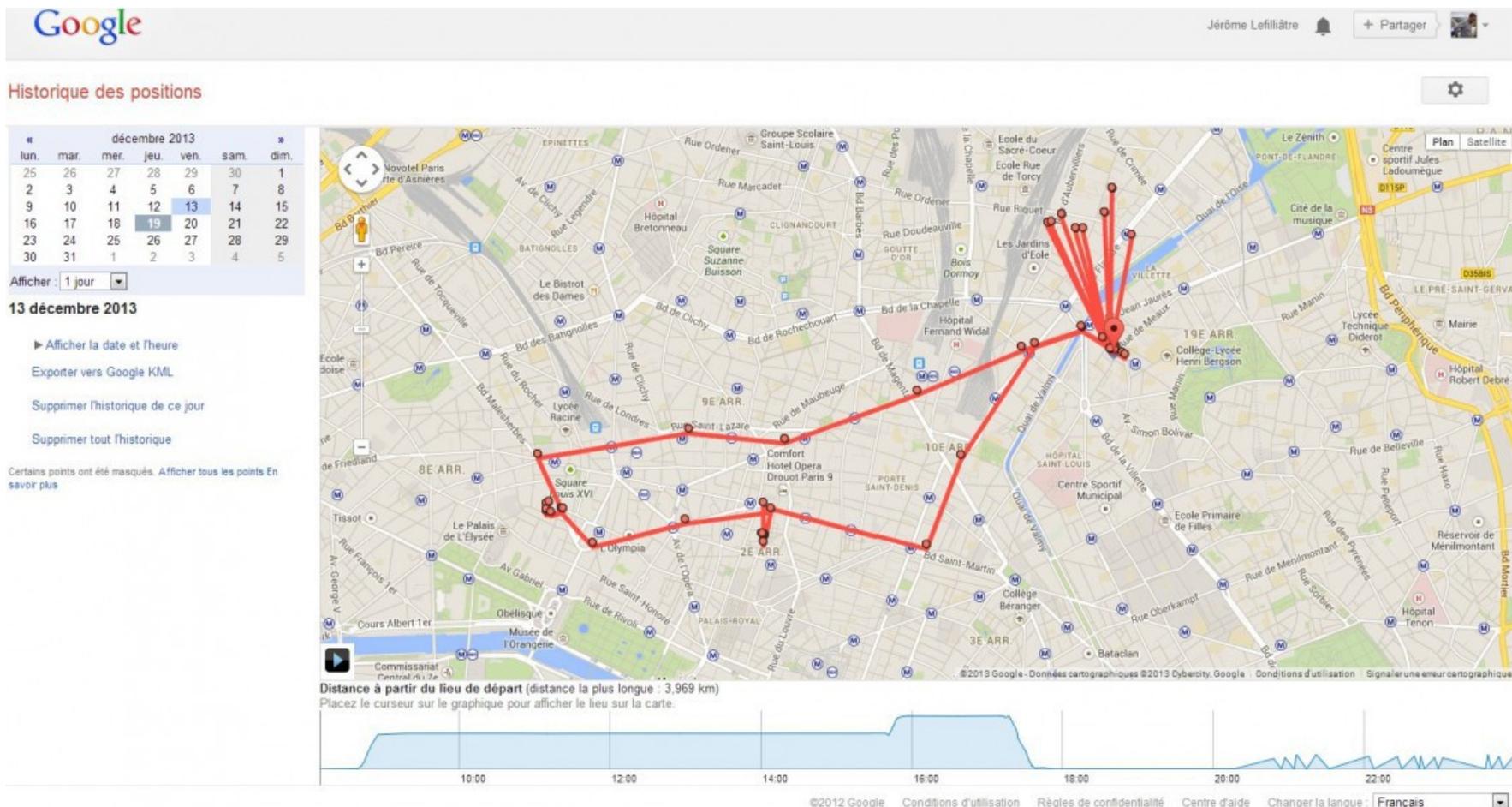


La Géolocalisation

- Tous vos déplacements sont enregistrés sur Android (versions 4 et ultérieures).
- Facebook projette de vous annoncer qui de vos contacts qui se trouvent à proximité.
- Désactiver les services de géolocalisation sur Android, ne les activer qu'en cas de besoin (GPS,...).

Le traçage par Google

- <https://maps.google.be/locationhistory/b/0>



Autres petits gestes

- Eviter les sites Flash (code non ouvert, backdoors potentiels,...).
- Déconnecter les sessions des réseaux sociaux lorsqu'on ne les utilise pas.
- Désactiver Wi-Fi, bluetooth s'ils ne sont pas utilisés.
- Utiliser moteurs de recherche alternatifs (duckduckgo).

Les réseaux sociaux

Réseaux sociaux : Règles essentielles

- Toute donnée sur un réseau social « propriétaire » doit être considérée comme publique.
- Vous êtes le produit que le réseau social vend à ses annonceurs (publicités, habitudes de consommation,... tout est enregistré).
- Les données mises sur ces réseaux ne sont plus sous votre contrôle.
- Un compte mal sécurisé et le monde entier est au courant de votre vie privée.

Le cas Facebook

- Facebook en sait plus sur vous que vous-même !
 - Contrôle toute vos communications, sms et mms avec Facebook Messenger (et rachat il y a quelques jours des messageries What's App).
 - L'anonymat n'est plus possible, chaque nouvel inscrit doit valider son compte avec téléphone ou envoi de copie de pièce d'identité.(voir slide suivant).
 - Comme beaucoup de réseaux, écoute votre activité sur internet (par exemple avec les boutons like ou la connexion sur site via Facebook,...).
 - Toute donnée effacée par l'utilisateur sont conservées.
 - Suggère la publicité selon vos goûts, habitudes,... et si vous n'aimez pas telle publicité vous demande quelle type d'annonce afficher :



Sponsorisé  Créer une annonce

Publicité masquée

Afin de nous aider à vous montrer de meilleures publicités, dites-nous ce que vous aimez.

Facebook © 2014
Français (France) · Confidentialité · Conditions d'utilisation · Cookies · Plus ▾

Autorisations de l'application

Facebook Messenger requiert les autorisations suivantes :

Communication réseau

Accès Internet complet

Stockage

Modifiez/Supprimez le contenu du stockage USB

Vos messages

Lire un SMS ou MMS, Modifier SMS ou MMS, Recevoir un MMS, Recevoir un SMS

Services payants

Envoyer un SMS, appeler directement des numéros de téléphone

Appels téléphoniques

Connaître état et ID

ACCEPTER

Pas d'anonymat

Veillez procéder à un contrôle de sécurité

Utilisez un téléphone pour valider votre compte

Le numéro de téléphone que vous utilisez ne peut confirmer qu'un seul compte. Lorsque vous aurez indiqué votre numéro, vous recevrez un code que vous pourrez saisir sur Facebook pour confirmer votre compte.

Votre numéro de téléphone sera ajouté à votre journal. Vous pourrez choisir à qui le montrer. Pour en savoir plus sur l'utilisation des informations de votre journal, consultez notre [politique de confidentialité](#).

Saisissez un numéro de téléphone

J'ai des problèmes avec cette étape.

▼ **Je n'arrive pas à confirmer mon compte à l'aide de mon numéro de téléphone.**

Si vous ne parvenez pas à confirmer votre compte à l'aide d'un numéro de téléphone mobile, vous pouvez envoyer une requête pour confirmer votre compte avec votre pièce d'identité officielle.

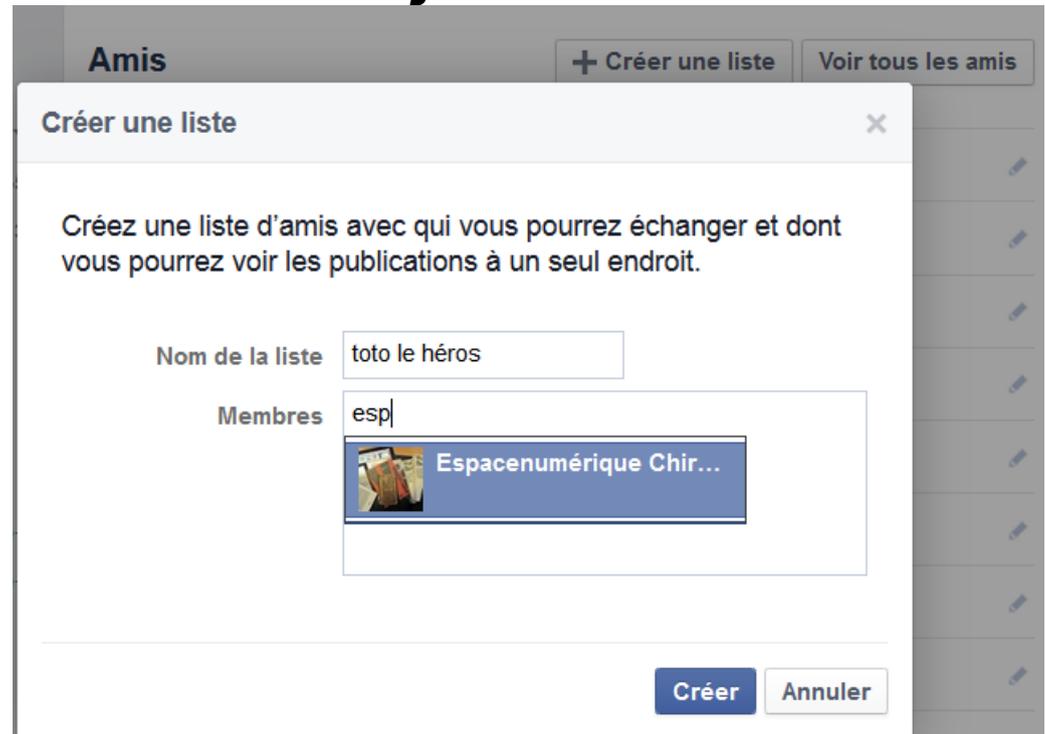
Vous lisez la réponse Aide de l'application de bureau. En savoir plus dans nos autres [pages d'aide](#).

Dernière modification il y a environ une semaine

Cloisonnement des publications

- Créer des listes pour cloisonner vos publications, photos, mentions j'aime...

Il est possible de paramétrer presque toute son activité sur Facebook avec les listes, ce qui permet de mieux contrôler nos données sur le réseau, nous verrons comment les utiliser dans les slides suivants.



Gérer la confidentialité

 Trouvez des personnes, des lieux ou d'autres choses

 Greg [Accueil](#)    

-  Général
-  Sécurité
-  Confidentialité**
-  Journal et identification
-  Blocage

-  Notifications
-  Mobile
-  Abonné(e)s

-  Applications
-  Publicités
-  Paiements
-  Espace Assistance
-  Vidéos

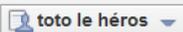
Paramètres et outils de confidentialité

Qui peut voir mon contenu ?

Qui peut voir vos futures publications ? [Fermer](#)

Vous pouvez gérer la confidentialité de ce que vous publiez à l'aide du sélecteur d'audience à **l'endroit même où vous publiez**. Votre choix est mémorisé et est appliqué dans le futur tant que vous ne changez pas d'avis.

Exprimez-vous

   toto le héros

N'oubliez pas – Il s'agit du même paramètre que ce dont vous disposez à l'endroit même où vous publiez. Tout changement est reflété aux deux endroits.

Examinez toutes les publications et tous les contenus dans lesquels vous êtes identifié(e) [Utiliser l'historique personnel](#)

Limiter l'audience des publications que vous avez ouvertes aux amis de vos amis ou au public ? [Limiter l'audience des anciennes publications](#)

Qui peut me contacter ?	Qui peut vous envoyer des invitations à devenir amis ?	Tout le monde	Modifier
	Quels messages doivent être filtrés dans ma boîte de réception ?	Filtrage de base	Modifier

Qui peut me trouver avec	Qui peut vous trouver à l'aide de l'adresse	Tout le monde	Modifier
---------------------------------	---	----------------------	--------------------------

Gérer les identifications et le journal

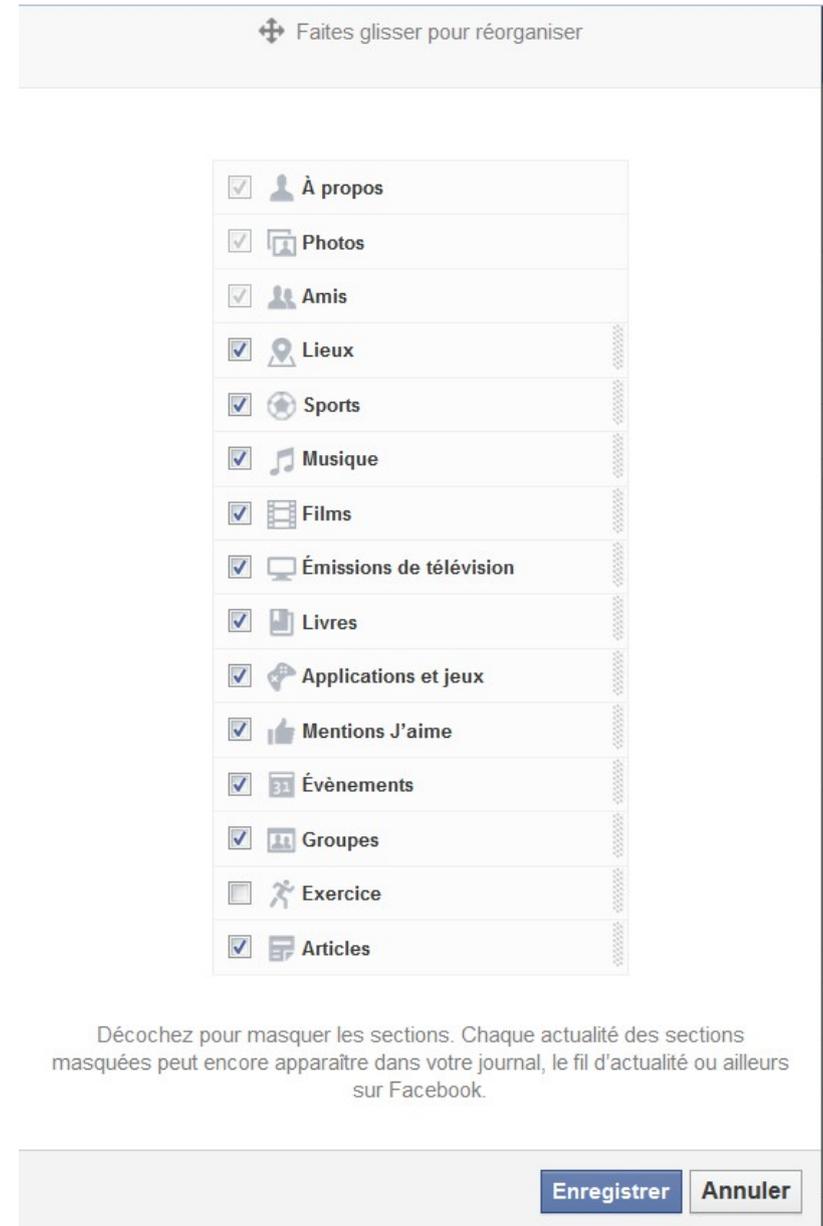
The screenshot shows the Facebook settings page for 'Paramètres d'identification et de journal'. A dropdown menu is open over the 'Amis' selection for the setting 'Qui peut voir les publications dans lesquelles vous êtes identifié(e) sur votre journal ?'. The dropdown lists various categories: Amis proches, Pirate, Région de Braine-l'Alleud, toto le héros, Namur, fnac, Famille, Suisse, VIP, Institut Cardijn, and Famille.

Paramètre	Description	Valeur	Action
Qui peut ajouter des contenus sur mon journal ?	Qui peut publier dans votre journal ?	Amis	Modifier
	Examiner les publications dans lesquelles vos amis vous identifient avant qu'elles n'apparaissent sur votre journal ?	Oui	Modifier
Qui peut voir les contenus de mon journal ?	Examinez ce que d'autres peuvent voir de votre journal		Afficher en tant que
	Qui peut voir les publications dans lesquelles vous êtes identifié(e) sur votre journal ?	Amis	Fermer
	Examinez ce que d'autres personnes publient sur votre journal	Amis	Modifier
Comment identifier une personne suggérée d'identification ?	Examinez les identifications que d'autres ajoutent à vos publications avant qu'elles n'apparaissent sur Facebook ?	Non	Modifier
	Quand un autre vous identifie dans une publication, souhaitez-vous ajouter à l'audience de la publication (vous n'avez pas encore accès à cette fonction) ?	Moi uniquement	Modifier
	Examinez vos suggestions d'identification lorsque vous semblez apparaître dans une photo téléchargée ? (vous n'avez pas encore accès à cette fonction)	Non disponible	

Gérer qui voit quoi



En cliquant sur le petit crayon sur les panneaux latéraux de gauche, nous pouvons paramétrer ce qui est visible sur le profil. Chaque petit panneau dispose de ses propres panneaux, nous nous arrêterons sur les like, en cliquant sur modifier la confidentialité.



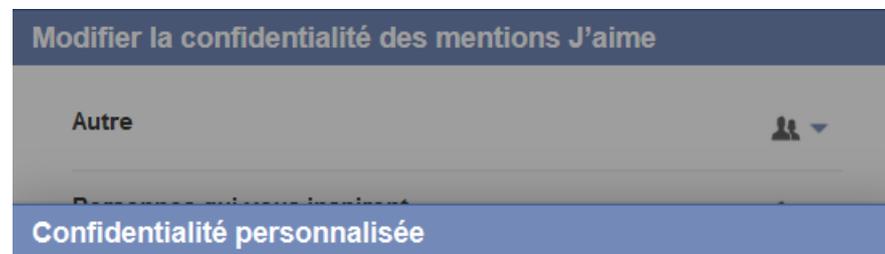
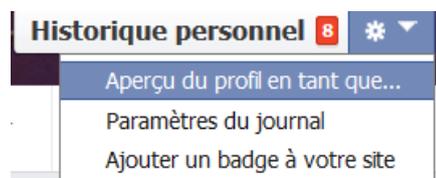
Décochez pour masquer les sections. Chaque actualité des sections masquées peut encore apparaître dans votre journal, le fil d'actualité ou ailleurs sur Facebook.

Personnaliser la confidentialité

Chaque catégorie des mentions j'aime est personnalisable. Pour cela, il faut choisir certaines personnes ou listes, et paramétrer comme bon vous semble.

Vous pouvez bien sûr vérifier ce qu'une personne voit (qu'elle soit dans vos contacts ou un simple visiteur).

Pour ce faire, cliquez sur le petit verrou près de votre photo de couverture et cliquez sur « Afficher le profil en tant que... »



✓ Ouvrir à _____

Ces personnes ou listes

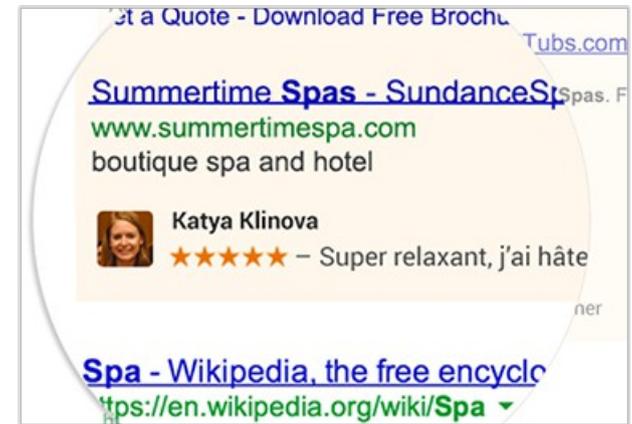
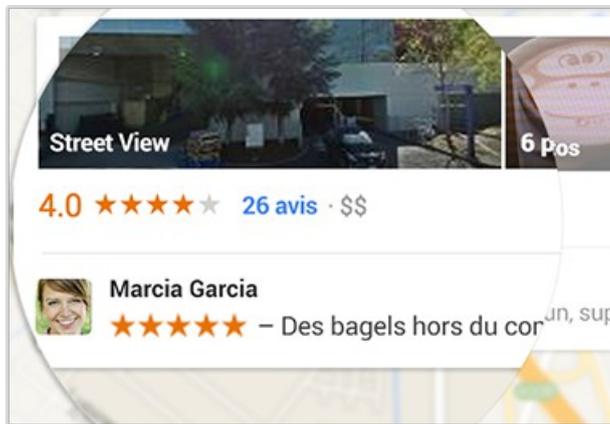
✗ Ne pas ouvrir à _____

Ces personnes ou listes



Google Plus

- Toute la confidentialité des listes de Facebook se font via les cercles et son utilisation beaucoup plus simple.
- Néanmoins, Google se réserve le droit d'afficher certaines de vos publications sur son moteur de recherche :



- Se désactive via une case à cocher en bas de page.

Solutions logicielles

Les solutions logicielles

- Le logiciel libre est la meilleure solution
 - Beaucoup de rapports sur des « backdoors » dans les produits Microsoft.
 - L'utilisateur n'a aucun contrôle sur le comportement d'une application propriétaire
 - Le code source d'un logiciel libre est accessible à tous, lisible et donc aisément modifiable en cas de besoin ou problème.
 - Une communauté active qui permet de corriger les bugs/problèmes de sécurité plus rapidement qu'un programme payant.

Changez vos applications !

Application propriétaire	Equivalent libre
Internet Explorer, Safari, Chrome	Mozilla Firefox, Chromium
M\$ Office	Open Office, Libre Office
Photoshop	The Gimp
3DS MAX	Blender
Skype	LinPhone, Jabber, Tox...
Mail, Outlook, Incredimail, Livemail,...	Mozilla Thunderbird
Appareils sous Android	Firefox OS ou Cyanogenmod
Windows et Mac OS	GNU/Linux ou FreeBSD (Unix libre)
Nero , cd burner	Géré nativement par les autres systèmes
Win Media Player, WinAmp,...	VLC

Extensions indispensables

- Petits ajouts pour un programme. S'installe en quelques clics.
- Accéder au centre d'applications de Firefox : bouton firefox -> Modules complémentaires

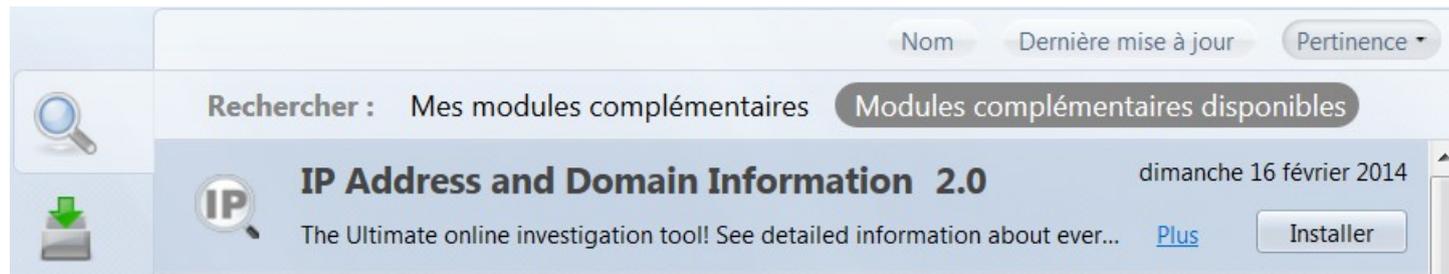


Extensions indispensables

- Adblock : bloqueur d'annonces publicitaires.
- Do Not Track Me / Mask Me : coupe les connexions qui regarde votre activité sur un site internet.
- LightBeam : Permet de visualiser en graphique qui espionne votre activité sur un site internet.
- Cryptocat : « chat » sécurisé et crypté du destinataire au destinataire.
- Foxy Proxy Basic : pratique pour gérer plusieurs proxies.

Installer une extension

- Dans le centre de contrôle des applications, rechercher l'extension désirée et juste cliquer dessus
- Une fois que la barre de progression arrive au bout, l'extension est installée (il se peut qu'un redémarrage du navigateur soit demandé pour que l'application fonctionne).

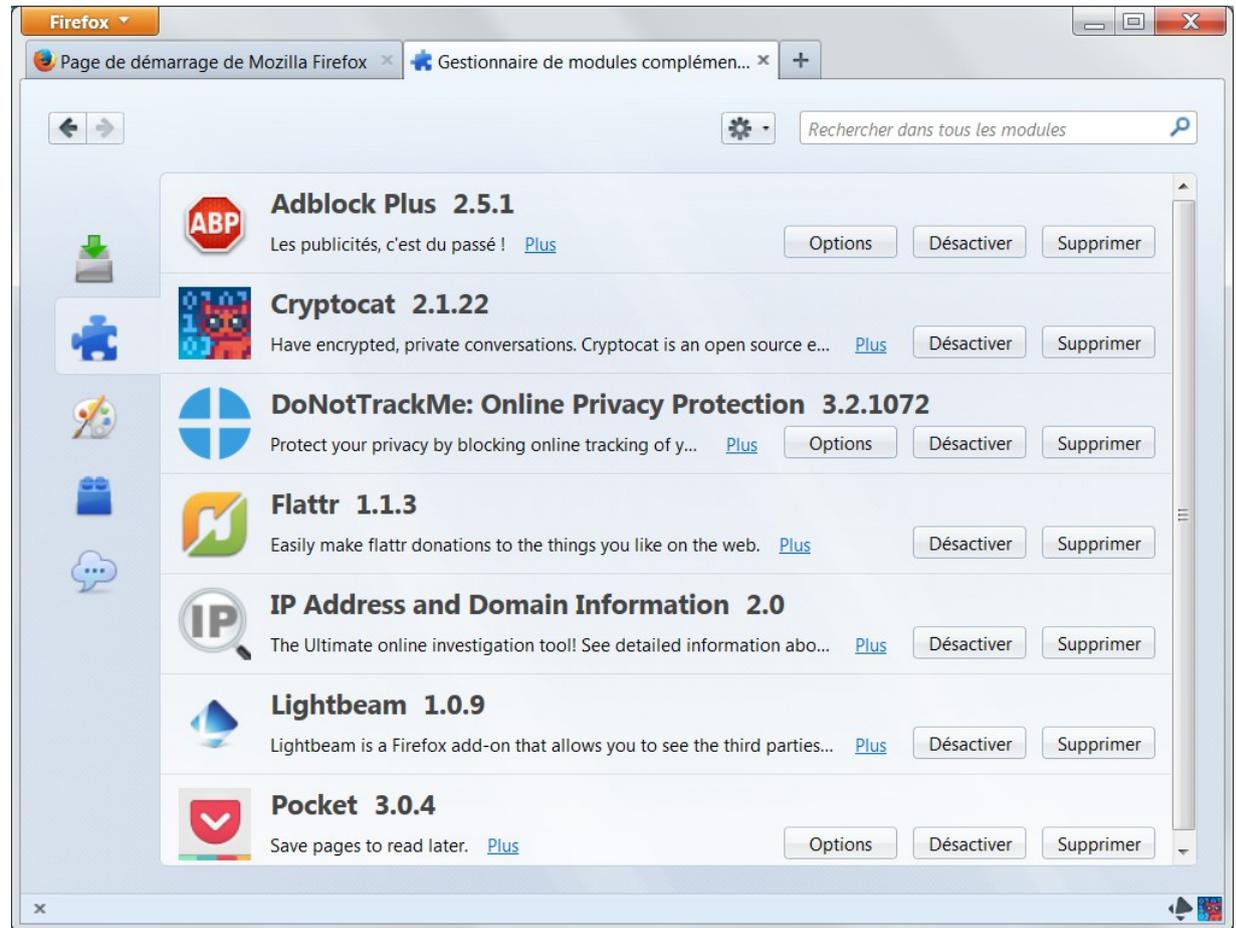


Gestion des extensions

Accès par la petite icône sous forme de pièce de puzzle.

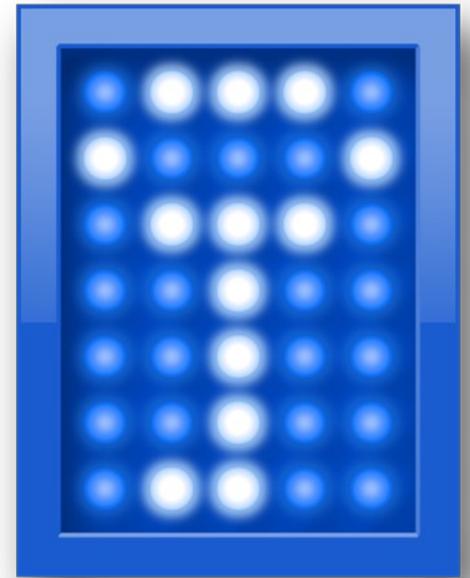
Les options de configuration des extensions s'y trouvent.

Désactivation et suppression des extensions.



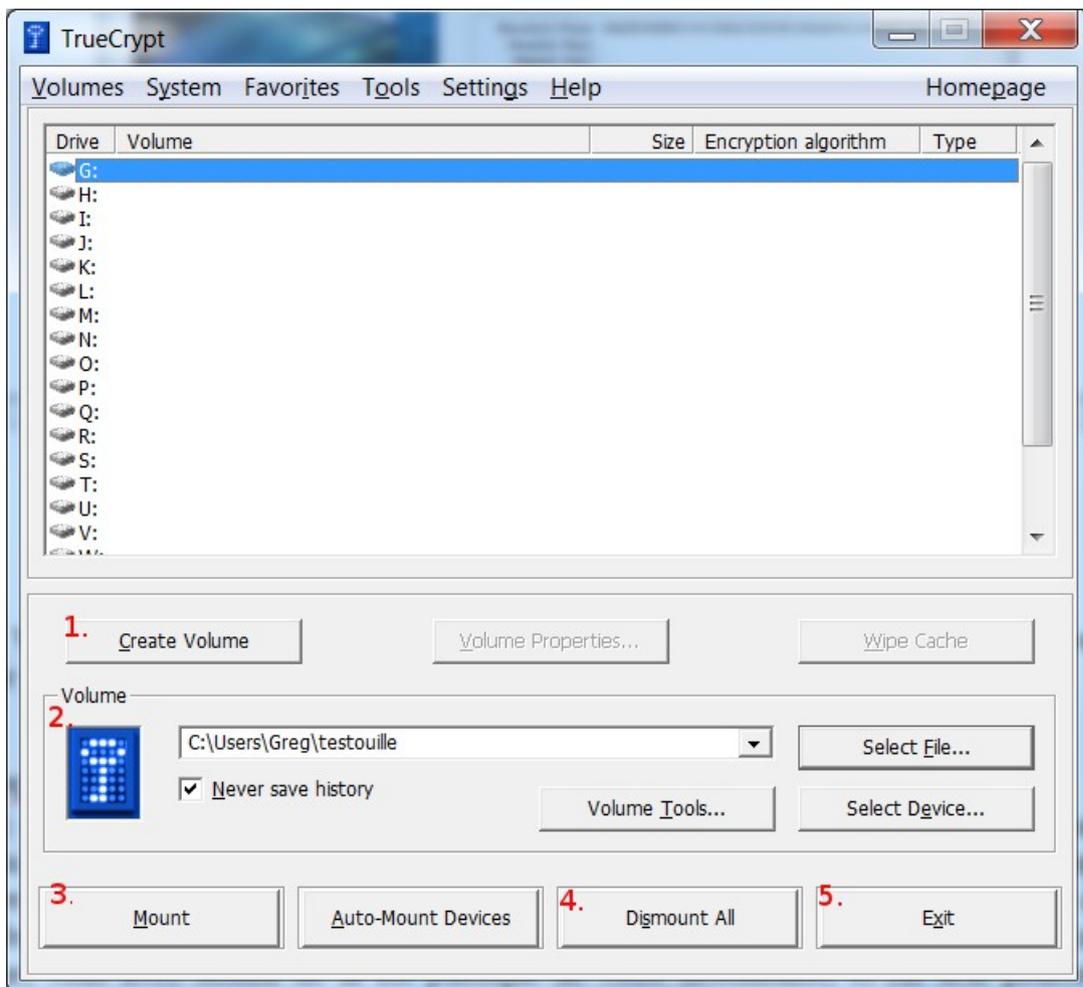
Truecrypt

- Permet de crypter des dossiers, containers, disques durs, clés USB ou systèmes entiers.
- Fonctionne sur tous les systèmes majeurs et rend les données facilement transportables.



Créer un dossier crypté - 1

L'interface d'accueil de Truecrypt sous Windows



1. Options pour créer le dossier crypté.

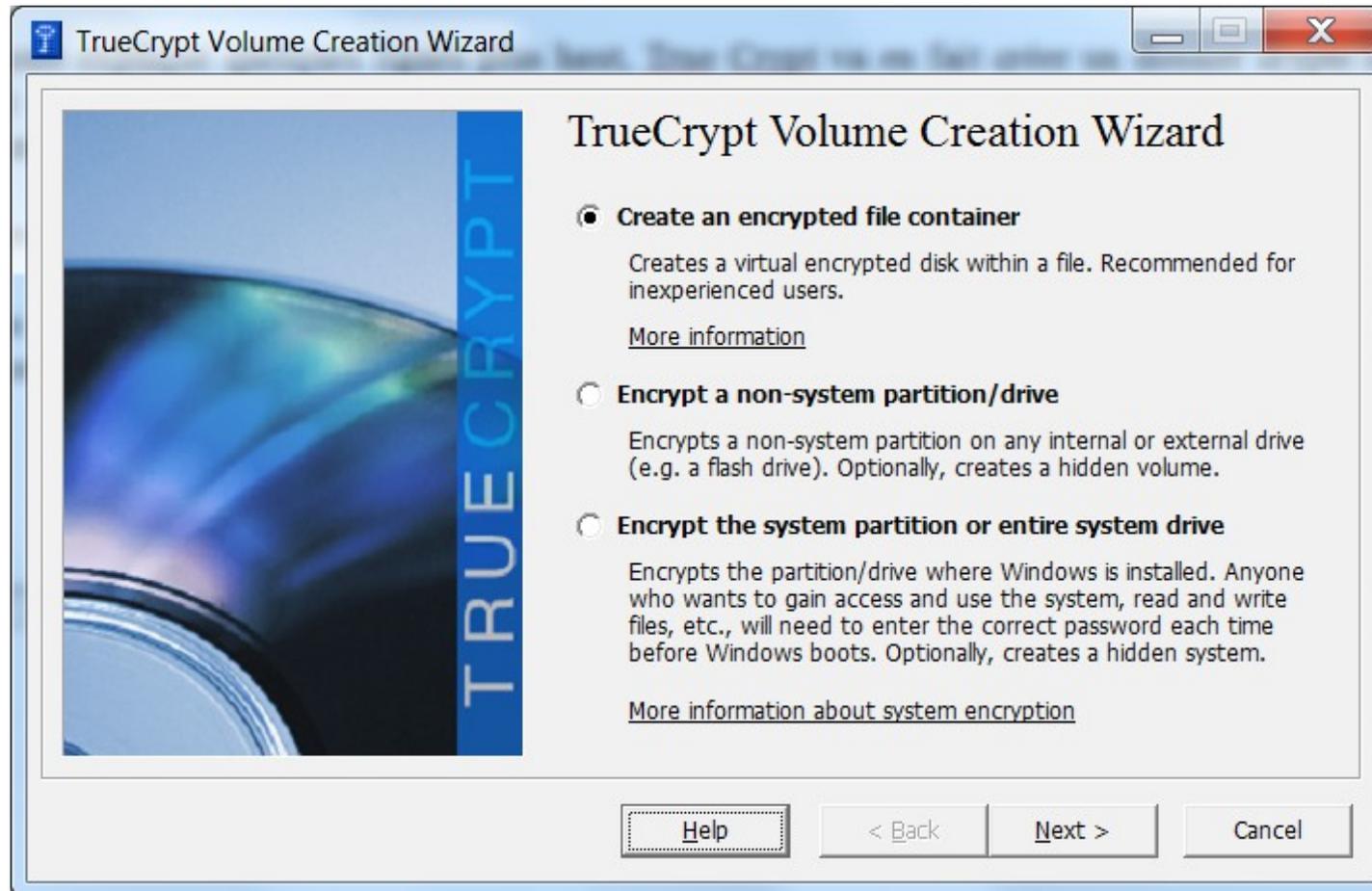
2. Options pour choisir le dossier crypté.

3. Monter le dossier crypté.

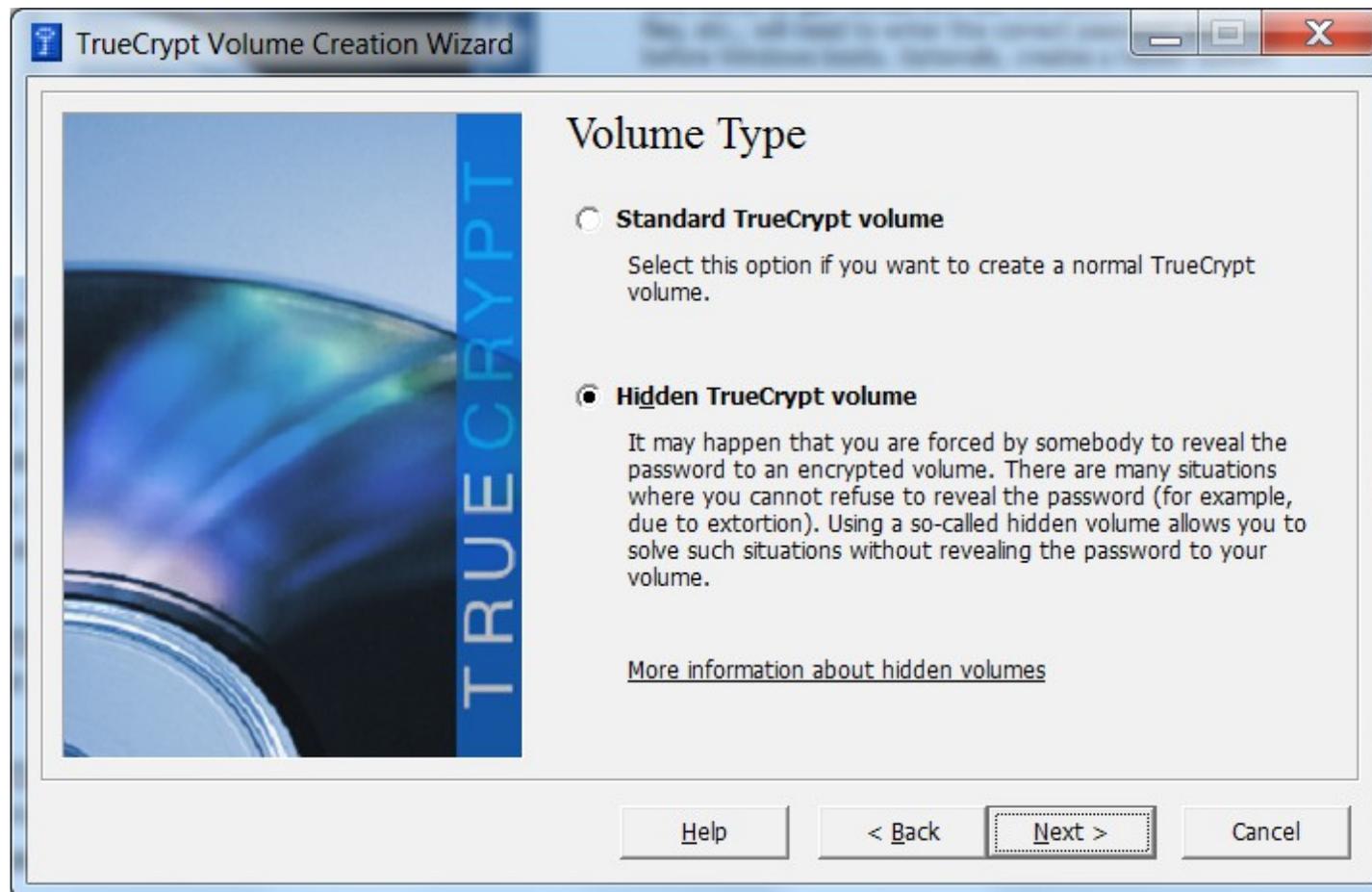
4. Démonter le dossier crypté.

5. Sortie du programme.

Créer un dossier crypté - 2



Choix du type du volume



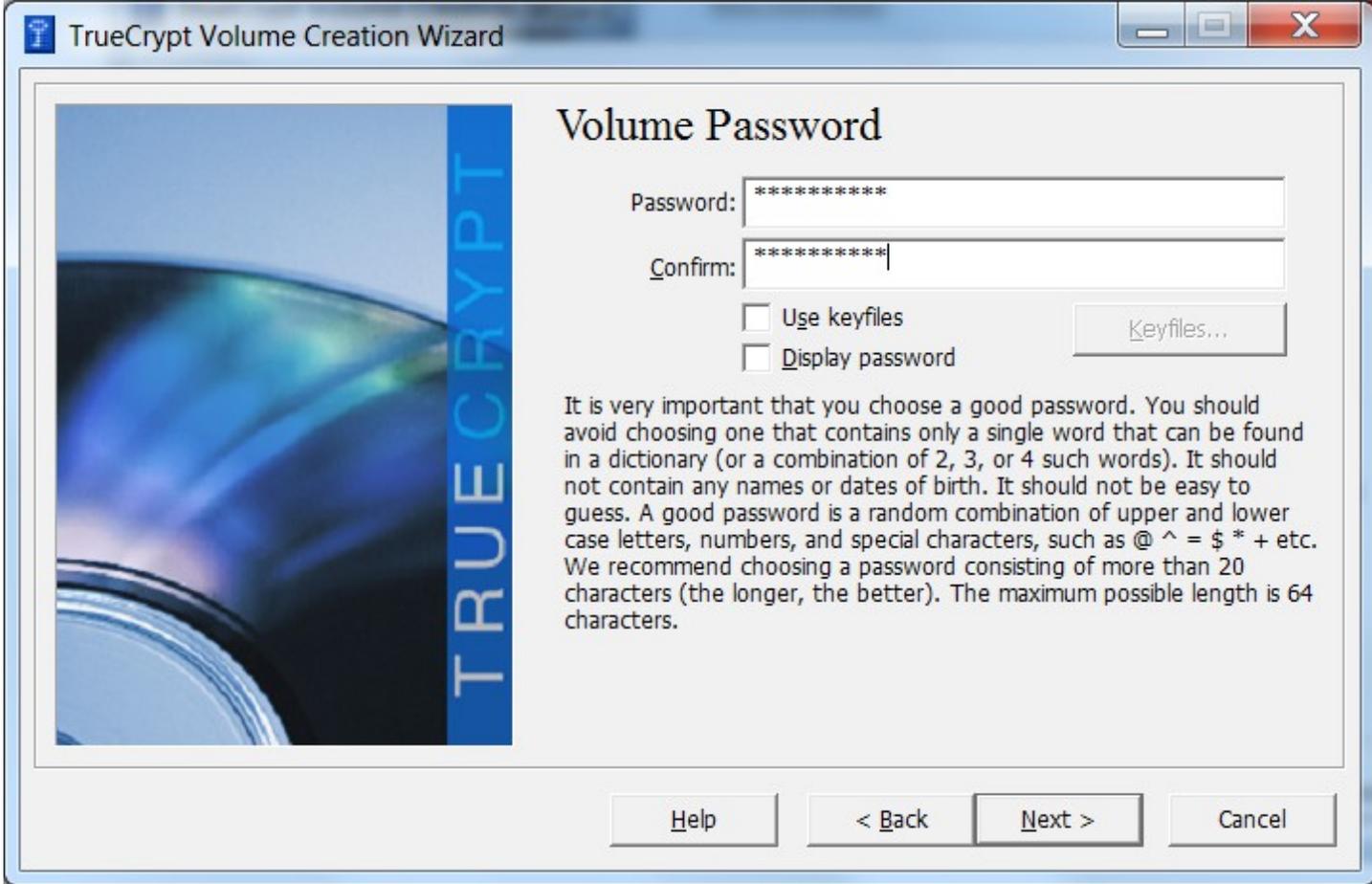
Méthodes de cryptage du dossier



Taille du volume



Mots de passe et clés



The image shows a screenshot of the TrueCrypt Volume Creation Wizard, specifically the 'Volume Password' step. The window title is 'TrueCrypt Volume Creation Wizard'. On the left, there is a graphic with the word 'TRUECRYPT' written vertically. The main area is titled 'Volume Password' and contains two text input fields for 'Password' and 'Confirm', both filled with asterisks. Below these fields are two checkboxes: 'Use keyfiles' and 'Display password', both of which are unchecked. To the right of the 'Use keyfiles' checkbox is a button labeled 'Keyfiles...'. A paragraph of text provides instructions on how to choose a good password, emphasizing length and complexity. At the bottom of the window, there are four buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

TrueCrypt Volume Creation Wizard

Volume Password

Password: *****

Confirm: *****

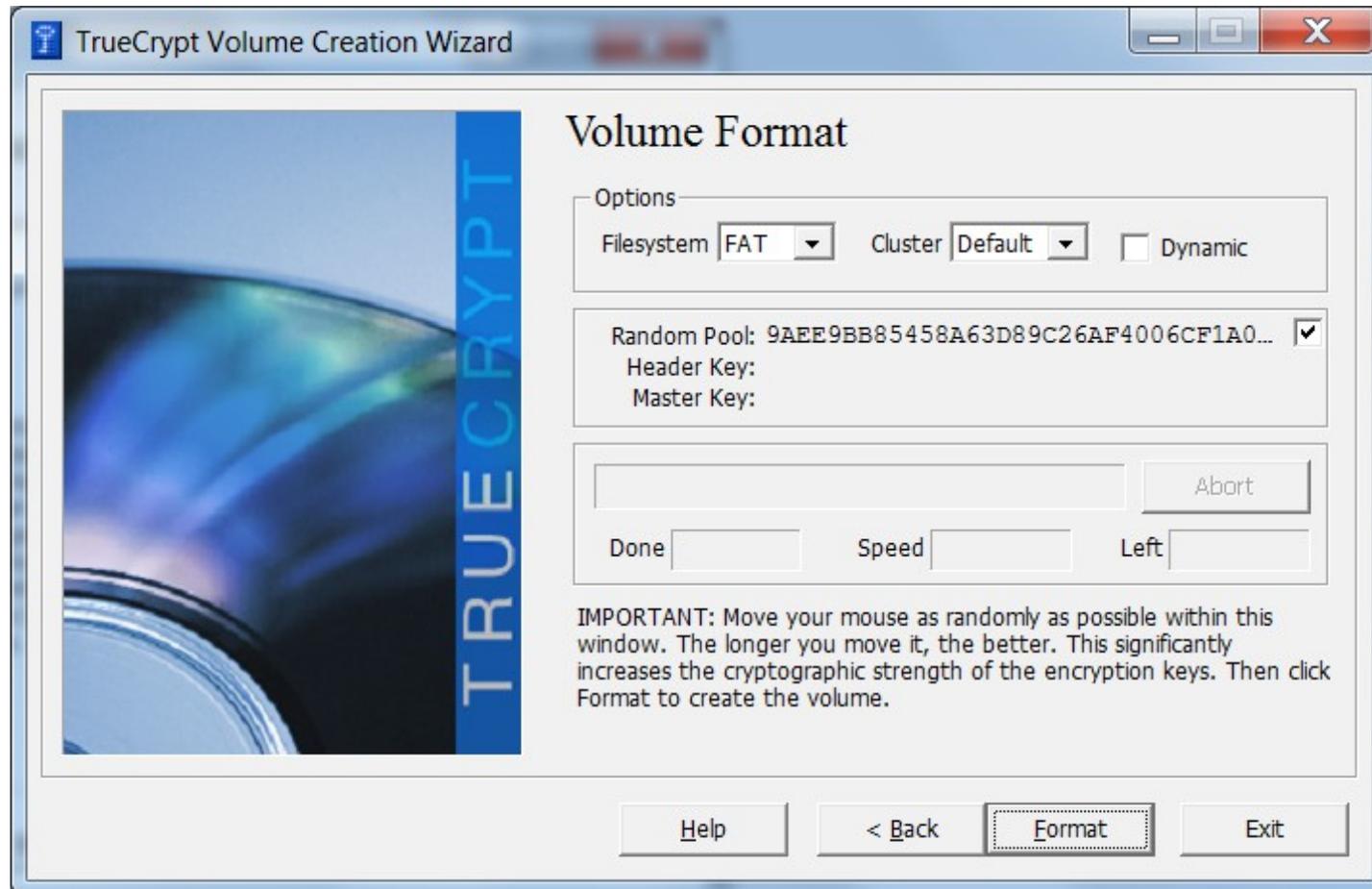
Use keyfiles Keyfiles...

Display password

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

Help < Back Next > Cancel

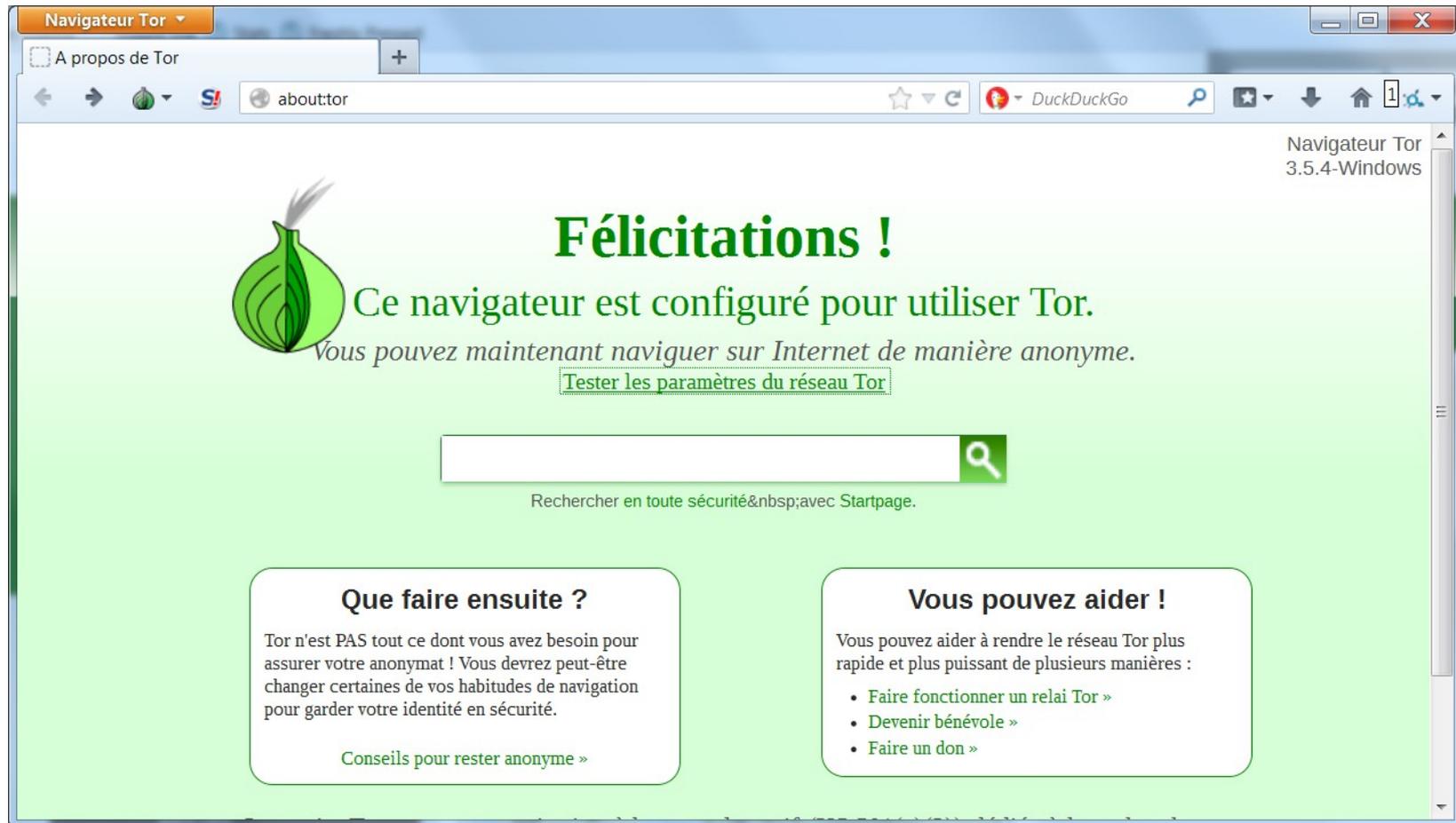
Formatage du Volume



Premiers pas avec TOR

- Utilisation du TOR Software Bundle, prise en main rapide.
- Basé sur Firefox avec différentes extensions, prévu pour fonctionner directement après installation.
- Renouvellement de son identité en un clic.

L'interface d'accueil



The image shows a screenshot of the Tor Browser's home page. The browser window title is "Navigateur Tor". The address bar shows "about:tor". The page features a green onion logo on the left. The main heading is "Félicitations !" in green, followed by the text "Ce navigateur est configuré pour utiliser Tor." and "Vous pouvez maintenant naviguer sur Internet de manière anonyme." Below this is a link "Tester les paramètres du réseau Tor". A search bar is present with the text "Rechercher en toute sécurité avec Startpage." Below the search bar are two boxes: "Que faire ensuite ?" and "Vous pouvez aider !".

Félicitations !
Ce navigateur est configuré pour utiliser Tor.
Vous pouvez maintenant naviguer sur Internet de manière anonyme.
[Tester les paramètres du réseau Tor](#)

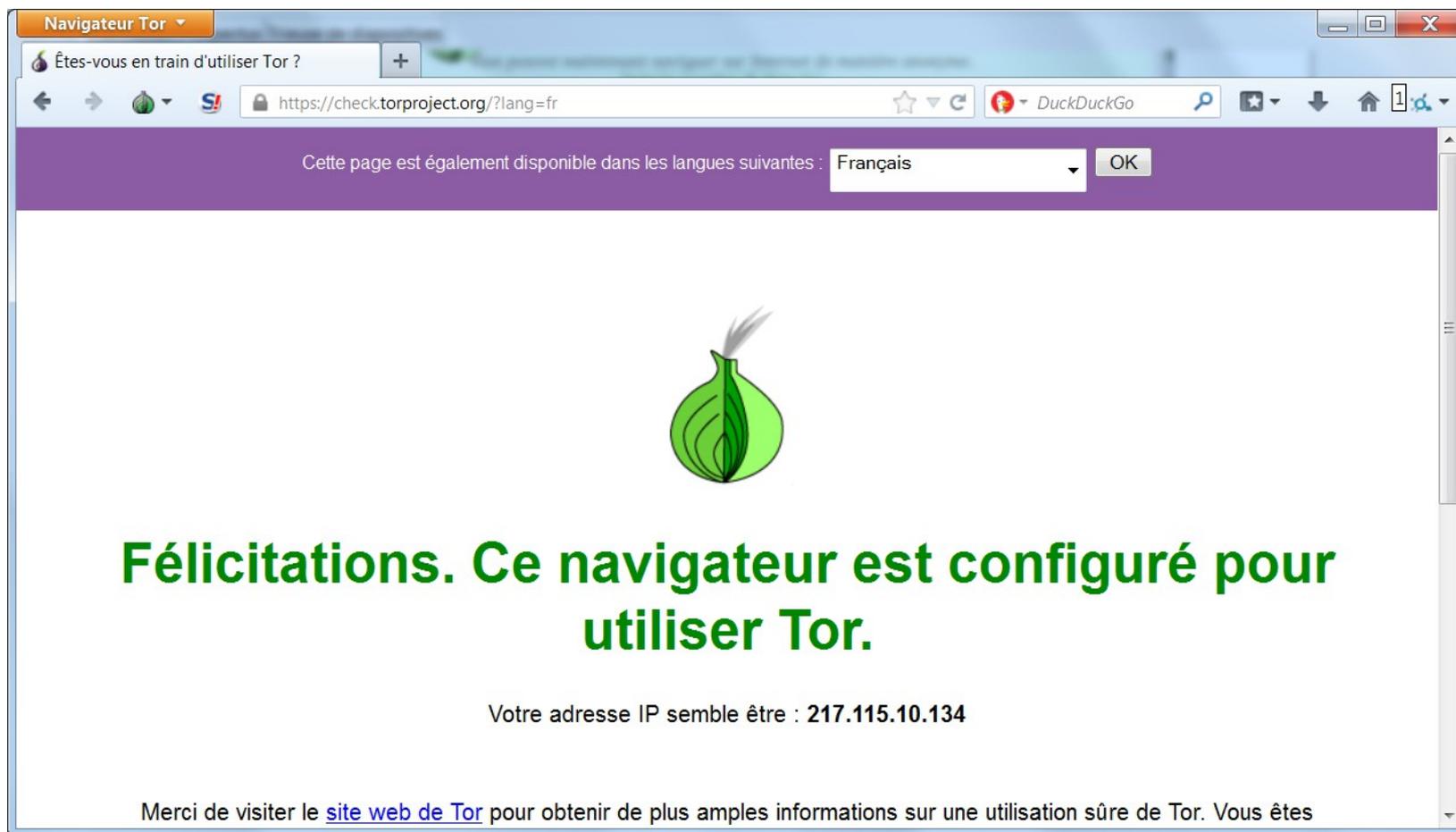
Rechercher en toute sécurité avec Startpage.

Que faire ensuite ?
Tor n'est PAS tout ce dont vous avez besoin pour assurer votre anonymat ! Vous devrez peut-être changer certaines de vos habitudes de navigation pour garder votre identité en sécurité.
[Conseils pour rester anonyme »](#)

Vous pouvez aider !
Vous pouvez aider à rendre le réseau Tor plus rapide et plus puissant de plusieurs manières :

- [Faire fonctionner un relai Tor »](#)
- [Devenir bénévole »](#)
- [Faire un don »](#)

Vérifier si ça fonctionne



On peut comparer avec votre ip réelle sur un navigateur en surfant sur le site www.whatismyipaddress.com

3 options essentielles :

- Le bouton oignon 
 - Changer d'identité.
 - Gérer les préférences et paramètres réseaux.
- Le bouton No Script 
 - Désactive Javascript.
- Le bouton Https Everywhere 
 - Ou c'est possible, forcer la connexion en https plutôt qu'en http (beaucoup de règles pré-faites).

Aller plus loin

- Cryptez vos mails avec GPG
 - <http://wiki.partipirate.org/wiki/Tutoriel:PGP>
- Utilisation des VPN
 - <http://samoht.fr/tuto/tuto-creer-un-serveur-vpn-sous-windows-gratuit-sans-installation>
- Rootage de votre appareil Android
 - <http://fsfe.org/campaigns/android/android.html>
- Passage sous Linux (Ubuntu est très facile pour les débutants et, une fois les premiers réflexes pris, est plus facile que Windows).
 - <http://www.ubuntu.com>

Aller plus loin : sensibilisation

- Sensibiliser votre entourage.
- Partage des outils et documents.
- Contacter votre MEP
(<http://www.respect-my-privacy.eu/fr>).
- Support des communautés libristes.

Liens et sources -1

- PRISM/XKEYSCORE
- http://www.lemonde.fr/technologies/visuel_interactif/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html
- [http://fr.wikipedia.org/wiki/PRISM_\(programme_de_surveillance\)](http://fr.wikipedia.org/wiki/PRISM_(programme_de_surveillance))
- <http://fr.wikipedia.org/wiki/XKeyscore>

- Législation sur les télécommunications en Belgique, septembre 2013 et directives européennes

- http://www.ejustice.just.fgov.be/cgi/article_body.pl?language=nl&pub_date=2013-10-08&numac=2013011510&caller=summary
- <http://eur-lex.europa.eu/legal-content/fr/ALL/;jsessionid=41yITWJDY9pXW0GBYQV0ny2V7dXGTYyrDVJPCTPQG6yVvDnT9wx8!1663640074?uri=CELEX:32006L0024>
- <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0058>

- Moteur de recherche alternatif

- <https://www.duckuckgo.com>

- La localisation avec Google

- <https://maps.google.com/locationhistory/b/0/>
https://support.google.com/gmm/answer/3118687?p=maps_location_settings&rd=1

- Le site officiel des cryptoparty

- <https://www.cryptoparty.in/>

Liens et sources -2

- Logiciels utilisés :
 - <http://www.truecrypt.org/>
 - <https://www.torproject.org/>
 - <https://adblockplus.org/fr/firefox>
 - <https://www.abine.com/index.html>
- Sites des associations promouvant le libre, la protection de la vie privée et la neutralité du net :
 - <http://www.nurpa.be/>
 - <http://fsfe.org/index.fr.html>
 - <https://www.april.org/>
 - <http://www.laquadrature.net/fr>
 - <http://www.framasoft.net/>
- Autres sources disponibles sur mon blog personnel :
 - <http://www.antredugreg.be/>

Téléchargements et contacts

- Twitter : @cappadocius
- About.me : <http://about.me/greg.siebrand/>
- XMPP : greg@xmpp.pirateparty.be
- Mail : g.siebrand@gmail.com
- Téléchargements :
<http://antredugreg.be/votre-vie-privee/>