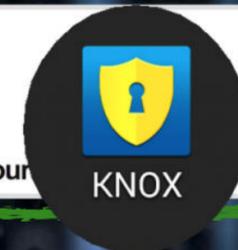


## Gestionnaires de mot de passe



## Conteneurs chiffrés



## Solutions de chiffrement pour la mobilité



## Protéger vos publications & éviter le tracking publicitaire

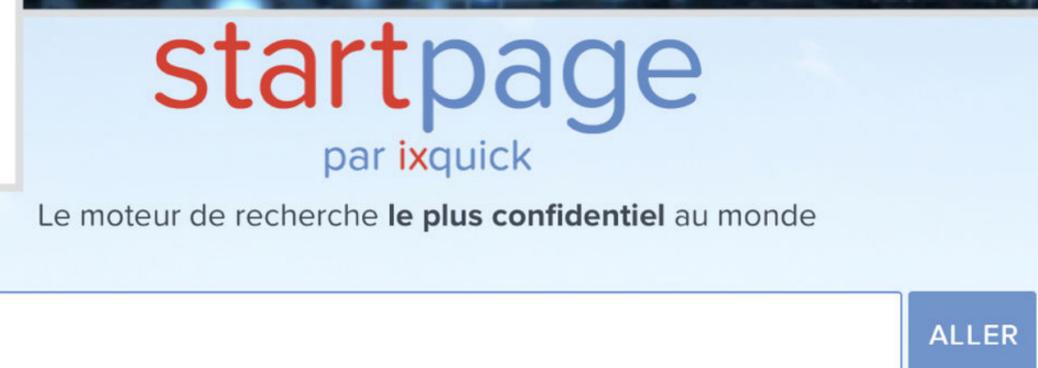
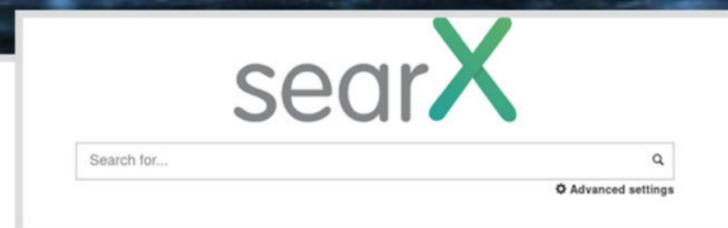
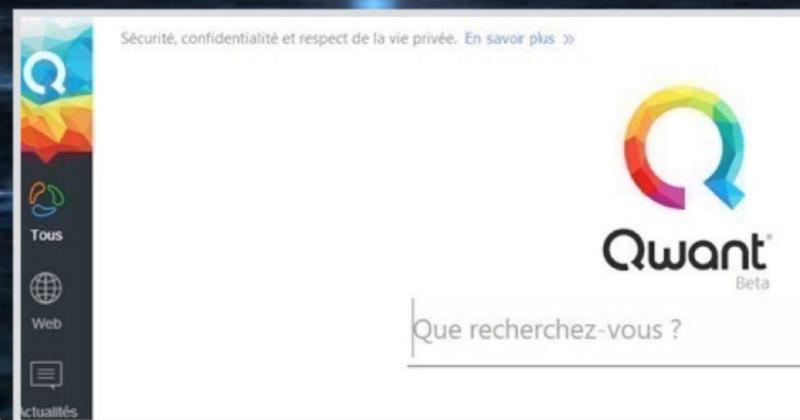


Privacy Badger

## Sauvergarde en ligne & détecteur de frappes



## Moteurs de recherche





**CYBERMALVEILLANCE.GOUV.FR**  
Assistance et prévention du risque numérique



Premier ministre

Agence Nationale  
de la Sécurité  
des Systèmes  
d'Information



Agence nationale de la sécurité  
des systèmes d'information

Que faire en cas d'incident ? | Le site du CERTA | Portail de la sécurité informatique



L'informatique doit respecter l'identité humaine, les droits de l'homme, la vie privée et les libertés



allo CNIL  
tél : 01 53 73 22 22

lettre info CNIL  
je m'inscris



Identifiant   Ok



**ELECTRONIC FRONTIER FOUNDATION**



MINISTÈRE  
DE  
L'INTÉRIEUR

**internet-signalement.gouv.fr**

Portail officiel de signalement des contenus illicites de l'Internet

**Internet Sans Crainte**

Donnons aux jeunes la maîtrise de leur vie numérique !

EDITION  
2018

**CATALOGUE  
DES SOLUTIONS  
QUALIFIÉES**

PAR L'AGENCE NATIONALE DE LA SÉCURITÉ  
DES SYSTÈMES D'INFORMATION



# LES FONDAMENTAUX DU VOYAGEUR

1

Garder ses documents de voyage avec soi (Passeport, boarding pass..) et laisser le minimum nécessaire dans sa chambre d'hôtel.

6

Garder vos appareils numériques sous surveillance et veiller à désactiver le Wifi et Bluetooth.

2

Utiliser un Vpn pour vos communications et favoriser les messageries instantanées plutôt que les emails pour les échanges.

7

Anticiper ce que vous allez partager comme information et chiffrer impérativement ses données.

3

Connaître la législation locale et son application. Choisir avec précaution le lieu où vous prévoyez d'échanger de l'information sensible.

8

Etre particulièrement discret dans les déplacements et dans sa communication.

4

En cas de rechargement de vos appareils connectés, utiliser exclusivement le câble Usb avec son chargeur.

9

Eviter de brancher des supports amovibles sur son PC, même s'il proviennent d'une personne que vous connaissez bien.

5

Avant le départ, effacer les données de navigation et laisser les appareils éteints au passage à la frontière.

10

Réduire au minimum son exposition aux réseaux sociaux et aux courriels. Se déconnecter des services une fois utilisés.

# SMART ATTITUDE(S) POUR SE PROTEGER...

2-Garder l'antivirus toujours à jour sur mon smartphone



3-Utiliser une messagerie anonymisée et chiffrée (chiffrement de bout en bout)

1  
Télécharger uniquement les applications proposées par des plate-formes officielles

4-Pour téléphoner en sécurité, opter plutôt pour la *messagerie instantanée*

CRYPTO SMART

Signal Private Messenger



wire



5-Utiliser en priorité *un VPN* pour me connecter à un Hotspot (Wifi public)