



Plusieurs dizaines d'ordinateurs, de smartphones déclarés volés ou perdus tous les ans au CNRS ...

Des données de la recherche, des données à caractère personnel ou liées à votre vie privée irrémédiablement perdues ! Pas pour tout le monde ?

## Protéger ses données contre la perte ou le vol ?

C'est très simple. Une action en deux temps

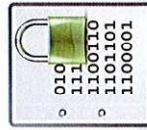
### 1. Sauvegarder

Régulièrement, mais pas n'importe où... Assurez-vous d'avoir toujours accès à vos sauvegardes, et de pouvoir les restaurer au besoin.



### 2. Chiffrer

Vous trouverez dans ce guide des éléments concrets de mise en œuvre du chiffrement sur vos équipements. C'est simple, efficace et sans risques.

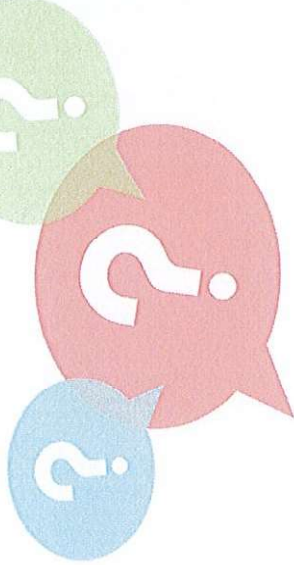


« Avant de prendre sa retraite, le directeur du renseignement américain, James Clapper, a dit que j'avais accéleré l'adoption du chiffrement de 7 ans [avec mes révélations]. Pour lui, c'était une insulte, mais je l'ai pris comme une sorte de compliment. »

- Edward Snowden, 2017

Des questions techniques ? Des problèmes de mise en œuvre ?

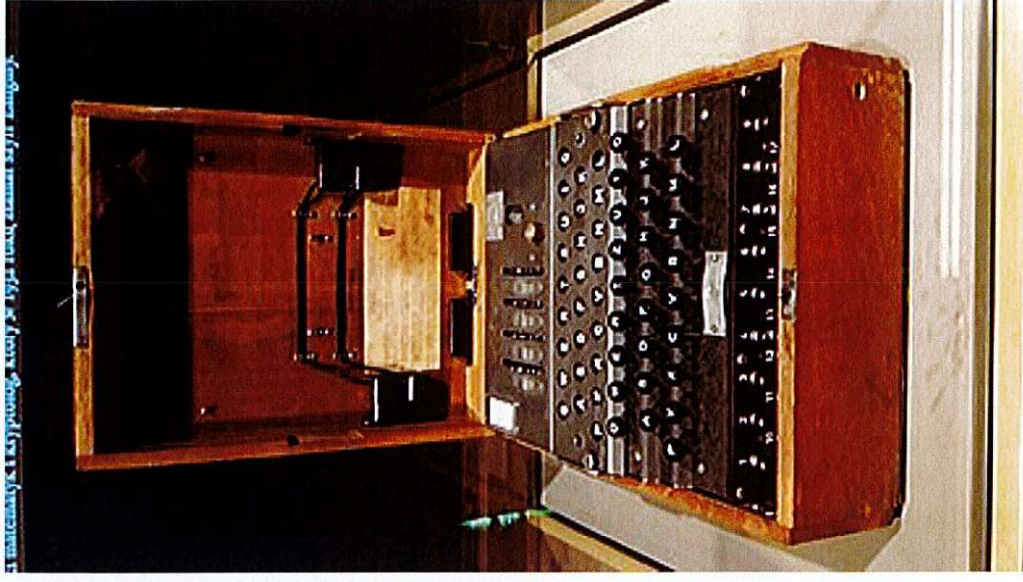
Prenez contact avec votre Chargé de SSI dans votre unité ou votre délégation.



Direction des Systèmes  
d'Information

Département Sécurité des SI

© 2018



# CHIFFREMENT DES TERMINAUX

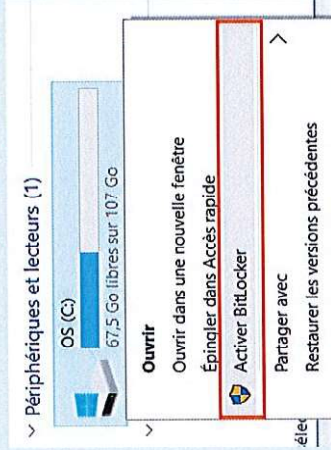
Vademecum





## Je travaille sous Microsoft Windows

A. J'utilise BitLocker intégré au système d'exploitation de mon PC...

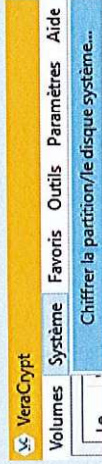


Dans mon explorateur de fichiers, je fais un clic droit sur mon disque système (C:) et je choisis « *Activer BitLocker* ».

Je sauvegarde ma clé de récupération sous forme d'un fichier PDF sur une clé USB, que je conserve sous clé.

B. ...ou j'utilise VeraCrypt, outil open-source de chiffrement « full disk »

J'installe et je lance le logiciel VeraCrypt [https://www.veracrypt.fr]. Je sélectionne les menus suivants. Je sauvegarde le disque de récupération sous forme de fichier ZIP sur une clé USB, que je conserve sous clé.



### Zone à chiffrer

- Chiffrer la partition système Windows**  
Sélectionnez cette option pour chiffrer la partition où le système d'exploitation Windows en cours d'utilisation est installé.
- Chiffrer l'intégralité du disque**

## Je travaille sous Apple Mac OS X

J'utilise FileVault intégré au système d'exploitation de mon ordinateur Apple



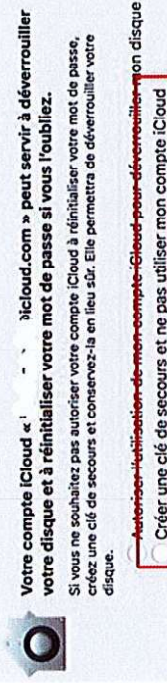
Je clique sur le menu Pomme > *Préférences Système*, puis sur *Sécurité et confidentialité*.

Je clique sur l'onglet *FileVault*.

Je clique sur le cadenas puis je saisis un nom et un mot de passe d'administrateur.

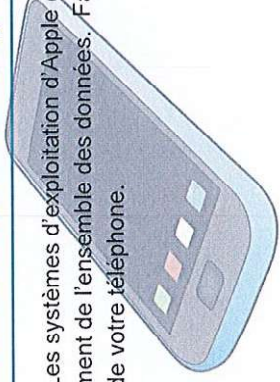
Je clique enfin sur *Activer FileVault*.

**ATTENTION:** En aucun cas je ne sauvegarde la clé de récupération sur mon compte iCloud! Je la sauvegarde sur une clé USB, que je conserve sous clé.



## Et sur mon smartphone ?

Les systèmes d'exploitation d'Apple (iOS) ou de Google (Android) permettent d'activer très simplement un chiffrement de l'ensemble des données. Faites un tour dans les options de sécurité de votre téléphone.



## Je travaille sous Linux (Fedora, Debian...)

Lors de l'installation de mon système, je choisis l'option de chiffrement de mes données.



### Partition disks

The installer can guide you through partitioning a disk (using different strategies), or you can do it manually. With guided partitioning you will still have a chance to customise the results.

If you choose guided partitioning for an entire disk, you will next be asked for the partitioning method:

Guided - use entire disk

Guided - use entire disk and set up LVM

Guided - use entire disk and set up encrypted LVM

Manual

