T2 - Effacer/cacher ses traces sur ordinateur

Vous pouvez consulter le sommaire sur la gauche, pour naviguer directement à l'endroit qui vous intéresse

Si vous avez des interrogations vis à vis de ce tutoriel, des choses que vous n'avez pas compris, ou par exemple des liens qui ne fonctionnent pas, n'hésitez pas à écrire un commentaire sur ce wiki, pour que nous puissions améliorer la compréhension de ce guide pour toutes et tous !

Les traces que nous laissons



Une des choses à faire en tant que rebel.le.s, si vous avez sur votre ordinateur des données potentiellement sensibles, relatives à votre activité de rebel.le, est de veiller à bien effacer les traces et données numérique que vous laissez sur votre ordinateur, ainsi que d'éviter d'en laisser, pour qu'elles ne puissent par être récupérées autrui.

En effet, lorsque nous utilisons notre ordinateur, nous laissons tout un tas de données sur ce dernier.

Ces données peuvent être de toute nature, il peut s'agir bien entendu de données liées à la navigation sur le web (navigateur, cookies, etc ...), dont nous montrons dans ce tuto comment s'en prémunir, mais il peut aussi s'agir d'autres données, comme :

- Des logiciels que vous avez installés/utilisés, qui laissent des traces même une fois désinstallés.
- Des « Journaux » donnant des informations sur ce qui s'est passé sur l'ordinateur, et potentiellement sur ce que vous avez fait dessus.
- De fichiers « supprimés », mais qui peuvent en réalité toujours être récupérés.
- Des méta-données de fichiers (je vous expliquerais de quoi il s'agit)
- Ou pire encore, directement des traces de données confidentielles liées à votre activité militante, comme des documents de planification d'action, des coordonnées, etc ...

Les guides

Pour vous prémunir de tout ces désagréments, ce guide sera divisé en 3 parties :

Effacer les traces de votre ordinateur :

Cas d'usage 1 :
Il y a, ou a eu, sur mon ordinateur, des données militantes comprométantes et/ou des logiciels compromettants, et je ne souhaite pas que les forces de l'ordre puissent les récupérer. Les données militantes ayant déjà été supprimées sont aussi concernées, si je ne les ai pas "réellement" supprimé avec un logiciel dédié (plus de détails dans le guide)
Chapitres concernés :
- "*Comment « réellement » supprimer vos données ?*"
- "*Comment « réellement » désinstaller nos logiciels*"

Cas d'usage 2 :
Dans le cadre d'une activité militante quelqonque, j'ai besoin de manipuler/envoyer des photos prises durant une action, et il faut que je m'assure qu'il n'y ait pas de métadonnées dans ces dernières contenant des informations potentiellement compromettantes permettant de remonter aux rebelles les ayant prises
Chapitre concerné :
- "*Effacer les méta-données*"

Guide ICI

Chiffrer vos données militantes :

Cas d'usage :
J'ai besoin, dans le cadre d'une activité militante quelquonque, de stocker des données sur mon ordinateur.
Ces données sont potentiellement compromettantes et je ne souhaite pas que les forces de l'ordre puissent les récupérer

Guide ICI

Utiliser une clé USB bootable :

Cas d'usage :
Maintenant que je sais mes données efficacement chiffrées et protégées grace à Veracrypt, j'ai besoin de cacher de manière générale le fait que j'utilise mon ordinateur pour une activité militante, car même avec les fichiers chiffrés, il existe toujours des traces de mon activité militante dans mon système d'exploitation (Windows, MacOS, etc ...)

Guide ICI

Créé 2023-09-10 13:42:51 CEST par mollusque
Mis à jour 2025-02-22 20:16:10 CET par mollusque