Soyez le/la propriétaire de vos fichiers

Author : Hélène Molinari

Date : 28 février 2017

Je suis une femme, j'utilise mon ordinateur et mon smartphone quotidiennement mais je ne maîtrise pas tous les outils qui sont à ma disposition pour faire en sorte d'être *vraiment* propriétaire de tous mes fichiers : documents, photos, vidéos, sons... Pourtant, on a tous en mémoire la diffusion de photos personnelles de stars inter-na-tio-nales sur les internets. Moins *people*, on connaît aussi le *revenge porn* et autres hacking de nos données. Il est temps de prendre les choses en main. Cette section du Guide DIY de cybersécurité féministe du collectif HACK*BLOSSOM nous aide à y voir plus clair.

#DATA

Vous êtes un-e cyberpunk technicien-ne averti-e : vos comptes sont sécurisés, votre navigation chiffrée et vous profitez d'internet depuis le confort douillet de votre VPN. Qu'arrive-t-il quand quelqu'un vole votre ordinateur ? Ou si votre service de cloud est hacké ? Et si cette super nouvelle application a un bug qui laisse les hackers télécharger vos données ?

Si vous avez des fichiers, des photos ou n'importe quel autre medium non chiffré, ce n'est PAS privé et vous devez supposer que quelqu'un ou quelque chose peut le voir.

Malheureusement, un des effets secondaires d'avoir autant de technologies extraordinaires à disposition est qu'on a trop confiance dans les développeurs et les compagnies qui les rendent possibles. On leur donne nos images, nos communications ou n'importe quelle donnée et on compte sur eux pour s'assurer que ça reste sécurisé. Alors que les hackers constituent une menace évidente et universelle, nous devons aussi considérer la possibilité qu'un développeur malveillant puisse lire nos données privées que nous envoyons sur son application. Que la surveillance gouvernementale puisse lire vos sms. Que quelqu'un qui vole votre ordinateur puisse deviner votre mot de passe et avoir accès à tout ce que vous avez sauvegardé sur le disque dur. C'est pourquoi le chiffrement est la clé : c'est la chose la plus sécurisée que vous pouvez faire pour garantir que vos données puissent être accessibles aux yeux que VOUS jugez nécessaires.

Avant d'expliquer les différentes façons de chiffrer vos données, cela peut aider d'expliquer ce qu'est le chiffrement. N'hésitez pas à sauter cette partie si vous savez déjà ce que c'est.

Qu'est-ce que le chiffrement ?

Le chiffrement empêche les personnes indésirables de lire vos données. Il le fait en les transformant en non-sens complètement incompréhensible pour que personne, sauf le destinataire choisi, ne puisse comprendre. C'est vraiment tout simplement un code secret. Comment ce code est-il créé ?

Le chiffrement en tant que tel regroupe des fonctions mathématiques dépendant de deux variables : vos données et un morceau d'information appelé la clé de chiffrement. Bien qu'il existe de nombreuses approches, la plupart du temps la clé de chiffrement a deux formes : la clé publique et la clé privée. Quand vous voulez chiffrer une donnée pour quelqu'un, vous utilisez leur clé publique pour la « verrouiller ». Quand cette personne veut lire la donnée chiffrée, elle utilise sa clé privée pour la « déverrouiller ».

Comment utilise-t-on ces clés ? Par exemple, disons que vous voulez envoyer un message privé à un ami par mail. Pour chiffrer vos données, vous les passez avec la clé publique de votre ami dans une fonction de chiffrement : ça produit un mélange de lettres et de chiffres appelé « texte-chiffré ». Si quelqu'un était amené à lire ce texte-chiffré, ce serait quasiment impossible de comprendre ce que ça signifie. Quand votre ami veut le lire, il passe ce texte-chiffré dans une autre fonction de chiffrement avec sa clé privée ; ce qui produit votre donnée originelle. Voyez-le comme mettre une lettre dans une boîte verrouillée : une fois que vous l'avez mise dedans, seule la personne qui a la clé peut l'ouvrir et lire la lettre.

C'est une explication hyper simplifiée, mais c'est tout ce dont vous avez besoin de connaître pour utiliser le chiffrement. La plupart des extensions et technologies citées dans les sections précédentes réalisent ce processus lorsque vous naviguez sur internet. Il existe aussi des applications qui peuvent le faire pour vos fichiers sur votre ordinateur. Cependant, si vous voulez chiffrer des textes dans un mail ou sur un Google doc, ou si vous ne voulez pas prendre le risque d'utiliser une application pour des fichiers locaux, vous pouvez les chiffrer manuellement avec des logiciels gratuits.

Préparez-vous au pire : chiffrez votre disque dur !

Disons qu'on vous vole votre ordinateur. Trop triste, les ordinateurs sont quand même chers :(

Il y a des chances que vous ne vouliez pas que certains fichiers sensibles se retrouvent entre les mains de ce connard-de-voleur. **Si vous chiffrez votre disque dur, ce connard-de-voleur ne pourra pas s'introduire dans votre ordinateur et voir toutes vos données !** Ce type de chiffrement fonctionne en chiffrant l'entièreté de votre ordinateur à chaque fois que vous l'éteignez. Quand vous le démarrez, vous devez entrer un mot de passe (on espère un fort!) pour déchiffrer le disque dur et le rendre utilisable. La chose importante à se souvenir est que ça ne protège que votre ordinateur s'il a été éteint ; si une personne malveillante a accès à votre ordinateur quand il est allumé, vos fichiers seront toujours vulnérables (il faudra chiffrer les fichiers avec un PGP pour ajouter un niveau supérieur de précaution).

Chiffrement du disque dur

OS X est fourni avec un logiciel, File Vault 2, déjà installé sur votre ordinateur et qui fera le chiffrement du disque dur pour vous. Tout ce que vous avez à faire est de l'activer en suivant les instructions d'Apple.

Windows 10 chiffrera votre disque dur par défaut, comme détaillé ici. Cependant, si vous avez une version antérieure de Windows, vous pouvez utiliser le logiciel Bitlocker.

Assurez-vous de vous rappeler votre mot de passe de chiffrement ! S'il vous arrivait de l'oublier, toutes vos données seraient irrémédiablement perdues. Il est aussi important de noter que bien que le chiffrement du disque dur soit un très bon moyen de dissuasion pour un voleur classique ou un troll essayant d'avoir physiquement accès à votre ordinateur, ce ne sera pas efficace contre un attaquant plus sophistiqué (comme une unité tech gouvernementale). Si ça vous inquiète, vous devrez chiffrer manuellement vos fichiers les plus importants avec un PGP.

Une chose très importante à garder à l'esprit est de faire des SAUVEGARDES. Bien sûr, c'est très bien de chiffrer votre disque dur, mais si votre ordinateur est volé, vous aurez quand même perdu vos données. Si vous sauvegardez votre ordinateur sur des disques durs externes, **assurez-vous de les chiffrer aussi**. Quel est l'intérêt de chiffrer votre ordinateur si quelqu'un peut juste emporter votre disque dur externe et avoir facilement accès à vos données privées ? Aucun ! Allez voir notre section "La tête dans le cloud" plus bas sur comment sauvegarder des fichiers sur un cloud chiffré.

Salissez-vous les mains : chiffrez vos fichiers et vos mails manuellement !

Pour les cyberpunks averti-e-s, être capable de chiffrer ses fichiers et mails est un atout fondamental. C'est particulièrement génial si vous voulez envoyer des informations privées à une autre personne dont vous avez *absolument besoin* qu'elle reste privée : un mail chiffré a l'avantage que seul le-la destinataire sera capable de voir le contenu, peu importe si le service

est surveillé. **Être capable de chiffrer manuellement un fichier signifie que vous avez un plus grand contrôle pour chiffrer des fichiers pour d'autres personnes (qui utilisent aussi le chiffrement), ou juste pour vous-même.**

Pretty Good Privacy

Pretty Good Privacy est une technologie que vous pouvez utiliser sur n'importe quel système d'exploitation pour chiffrer vos mails et fichiers, pour signer une donnée (en gros, ajouter une signature numérique prouvant que vos clés de chiffrement ont été utilisées correctement) et pour vérifier les signatures (s'assurer que la signature de quelqu'un d'autre est honnête). C'est une installation un peu plus avancée, mais pas si difficile si vous avez une heure et quelque et un peu de patience à tuer. Une fois fini, le chiffrement de mails et de fichiers sera un jeu d'enfant !

Il est fondamental de prendre en compte ce qu'il se passerait si vous perdiez vos clés de chiffrement (par exemple si votre ordinateur est volé ou cassé) : tout ce qui aura été chiffré sera perdu à jamais. Si vous avez des fichiers ou des mails que vous devez chiffrer et rendre accessibles qui ne doivent absolument pas être perdus, vous devez faire une sauvegarde de vos clés. Depuis n'importe quel programme PGP que vous avez installé, vous devriez avoir une option d'export de vos clés. Sauvegardez-les sur une clé USB et gardez-les dans un endroit incroyablement sécurisé.

L'Electronic Frontier Foundation offre des guides détaillés pour installer PGP sur OSX et Windows.

La tête dans le cloud : sauvegardez vos fichiers sur un cloud chiffré !

Il y a de grandes chances que vous utilisiez des services comme Dropbox ou Google Drive pour synchroniser vos fichiers sur le cloud. Bien qu'ingénieux, ces services sont susceptibles de partager vos fichiers à des « parties intéressées » en cas d'obligations légales. Et s'ils étaient hackés, tous vos fichiers seraient accessibles à tous sur internet. Comme la plupart des choses dans la vie, ces services sont bien meilleurs lorsqu'ils sont chiffrés : si les fichiers le sont sur le cloud, et déchiffrés sur votre ordinateur, vous aurez les mêmes fonctionnalités que Dropbox ou Google Drive sans les risques de sécurité !

Il existe de nombreux services qui offrent un stockage chiffré sur cloud. Jetez un œil au guide de services de cloud réalisé par Lifehacker pour déterminer ce qui vous convient le mieux.

CONSEIL SÉCURITÉ : Assurez-vous de TOUJOURS sauvegarder vos fichiers localement en plus de les synchroniser avec le cloud. Si votre service de cloud meurt soudainement pour n'importe quelle raison, vous serez terriblement vulnérable (et votre ordinateur sera probablement volé la même semaine parce que le monde est cruel). Sauvegardez vos fichiers les plus importants sur un disque dur externe, que vous devriez *définitivement* chiffrer aussi (comme détaillé dans les sections précédentes : #ANONYMAT #HACKING).

#INTRODUCTION

#ANONYMAT

#HACKING

#TÉLÉPHONES

#SOCIAL

#CHEAT SHEET