Ne laissez pas les trolls voir vos pensées intimes et vos expériences

Author : Hélène Molinari

Date : 5 mars 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 que toute ma vie sur le net ne soit pas à la portée de tout le monde (et surtout n'importe qui)... Et pourtant, je continue de poster sur Facebook en public sans me demander qui pourra lire mes propos. J'y mets mes photos de vacance. Je "like" des photos des gamin-e-s de mes ami-e-s. Tous mes comptes sont connectés entre eux, permettant au premier ou à la première venue de se balader très facilement entre mes tweets, mes posts et autres com'. 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.

#SOCIAL

Annonce : cette section considère que vous avez lu ou consulté les parties précédentes (#ANONYMAT #HACKING #DATA #TÉLÉPHONES) et que vous vous êtes déjà emparé-e des techniques de base de la sécurité comme la double authentification, les mots de passe forts, les extensions de navigateurs, le chiffrement de téléphone et le chiffrement d'ordinateur. Tous ces points sont particulièrement importants pour protéger vos communications et votre activité sur les réseaux sociaux, mais nous n'allons pas y revenir ici en détails.

On se socialise sur internet. On se fait des amis sur les réseaux sociaux, on s'organise et on y planifie notre vie, c'est le lieu principal de nos communications. Puisque tout cela est possible grâce à différentes compagnies dans un réseau élaboré (facilement accessible à la surveillance gouvernementale), **il est quasiment impossible de garantir que votre vie reste vraiment privée si vous vous fiez uniquement à ces compagnies privées pour vous connecter à vos amis en ligne**. Les développeurs, travailleurs IT, marketers et un nombre incalculable de personnes peuvent voir vos messages et médias les plus intimes. Et parce que la plupart de ces compagnies stockent les métadonnées indéfiniment, vos conversations d'aujourd'hui et de demain peuvent encore être menacées des années plus tard.

Nous allons d'abord vous guider à travers des suggestions pour savoir comment exploiter les options de sécurité sur les différentes plateformes de réseaux sociaux. Même mieux, nous allons explorer des alternatives gratuites et open source de chats et mails pour que, lorsque vous en avez besoin, vous puissiez vraiment avoir des conversations privées qui peuvent résister aux hackers les plus déterminés et à la surveillance.

Prenez connaissance de la sécurité sur vos réseaux sociaux

La première étape pour sécuriser votre vie sociale numérique est de simplement prendre connaissance des options de privacité et de sécurité qui sont disponibles. Bien que ces options n'arrêteront pas les pro du marketing, les développeurs sans scrupules ou la surveillance gouvernementale d'accéder à vos données, elles pourront le rendre beaucoup plus difficile pour un troll inexpérimenté qui tenterait de vous hacker ou de vous agresser. Parce que les options de sécurité et les stratégies peuvent varier de façon significative entre les plateformes, nous allons vous présenter quelques points de base que vous devriez garder en tête quand vous utilisez un réseau social.

Prenez garde aux hameçonnages et autres ingénieries sociales

L'ingénierie sociale, la manipulation psychologique des cibles, est de loin la façon la plus répandue de hacker un compte sur un réseau social. Prenez connaissance de l'ingénierie sociale dans notre section sur le hacking pour être conscient-e de ces types de menaces ! En gros, **ne donnez jamais votre mot de passe à qui que ce soit, ne vous connectez jamais sur votre compte à partir d'un lien ou d'un site dont vous n'êtes pas familier-ère et essayez de ne pas utiliser vos comptes pour vous connecter à d'autres sites.** Ne vous connectez que via le site officiel dans votre navigateur ou via les applications officielles.

Utilisez la double authentification et des mots de passe forts

Hacker un compte de réseau social est très facile si celui-ci ne requiert qu'un simple mot de passe. Mais c'est aussi très simple à éviter! Si vous avez mis en place une double authentification et un mot de passe fort (comme détaillé plus tôt dans ce guide), un troll malveillant aura besoin d'un ordinateur extrêmement puissant ET d'un accès personnel à votre ordinateur/téléphone, de façon simultanée. Parce que ces technologies sont très faciles à mettre en place, elles font sans aucun doute partie des meilleures étapes à suivre pour protéger vos réseaux sociaux.

Méfiez-vous de la géolocalisation

De nombreux services sur les réseaux sociaux se servent des données GPS de votre téléphone ou de l'adresse IP de votre ordinateur pour associer un lieu physique à vos publications. Cette information est souvent librement exposée aux développeurs, c'est-à-dire que n'importe qui pouvant voir vos publications peut facilement trouver des informations sensibles sur votre lieu de vie ou vos habitudes de trajets. De nombreux sites, comme Twitter, offrent la possibilité de désactiver la géolocalisation dans les paramètres de sécurité, donc cherchez cette option sur tous les sites sur lesquels vous postez du contenu ou des médias. Une solution plus complète (mais aussi plus avancée) est d'utiliser un Réseau Privé Virtuel (VPN) pour que toute votre activité apparaisse comme provenant d'un data center au hasard, quelque part dans le monde.

Ne vous fiez pas aux applications qui demandent un accès à votre compte

C'est très habituel d'utiliser des applications dans le réseau social lui-même (par exemple une application Facebook) et en-dehors du site (par exemple, une fonctionnalité de Snapchat). Cependant, quand vous vous enregistrez pour ces applications, vous devez souvent exposer des tas de données personnelles : votre identité, vos photos, vos messages, vos amis. Si ça ne vous semble pas si grave, ça veut dire que vous faites confiance à des développeurs avec des informations profondément personnelles. **De nombreux services d'applications sont créés par des programmeurs inexpérimentés qui n'ont pas les ressources adéquates pour protéger vos données (s'ils s'en soucient).** La majeure partie du temps, ils veulent juste récolter vos informations pour les revendre aux agences de marketing. Sauf si vous avez vraiment, vraiment besoin de cette application, reconsidérez le fait que des inconnus puissent voir tout ce que vous faites sur les réseaux sociaux.

Familiarisez-vous avec les paramètres de sécurité de vos sites

Chaque site a ses propres capacités de sécurité, certaines plus complètes que d'autres. Vous devriez jeter un œil à ces rapides guides de vos sites préférés et comprendre quels outils vous avez à disposition.

- Facebook
- Twitter
- Instagram
- Snapchat
- Tumblr

- LinkedIn

Utilisez un chiffrement super fort pour votre messagerie avec Signal

Il est très courant d'utiliser une messagerie comme Facebook ou Google Hangouts pour parler avec des amis : vous pouvez utiliser assez facilement le même service sur différents appareils et toujours avoir accès à vos conversations. Malheureusement, celles-ci font l'objet d'une intense collecte de données par les publicitaires et les agences gouvernementales. Et si quelqu'un était amené à hacker ou faire fuiter votre compte, on pourrait voir des années et des années de conversations privées parce que les données ne disparaissent jamais.

Par chance, il existe de super alternatives open source, sécurisées et gratuites aux services de messagerie standards des grandes compagnies. **Signal est une application pour chiffrer vos sms pour que le contenu de vos messages ne puissent être vu par personne d'autre que vous-même et la personne avec qui vous parlez.** On peut l'utiliser pour des messages entre deux personnes, en groupe ou même des appels téléphoniques.

Jetez un œil à notre section sur Signal pour vous y mettre !

Protégez vos conversations par mail avec PGP

Le chiffrement standard pour sécuriser les communications est de facto PGP, que vous avez déjà vu dans la section sur les données (vous devriez peut-être revenir en arrière et lire comment le chiffrement fonctionne puisqu'on ne va pas le répéter ici). Un mail est constamment contrôlé par les services (c'est pour ça qu'ils sont gratuits après tout). **PGP, qui signifie Pretty Good Privacy, vous permet de chiffrer vos mails (et à peu près tout le reste) avec un niveau très haut de sophistication**. Ce qui est préférable aux messageries instantanées parce que :

1. Le destinataire a besoin d'utiliser un mot de passe pour déchiffrer tout ce que vous lui envoyez, donc c'est considérablement plus dur pour un voleur ou un hacker d'accéder à votre mail.
2. Vous pouvez « signer » numériquement votre mail, ce qui permet de mieux prouver que c'est bien vous qui l'avez écrit.
3. Vous pouvez toujours trouver les clés publiques de quelqu'un (ce dont vous avez besoin pour chiffrer un message pour eux) en ligne, ce qui vous permet très facilement de chiffrer des éléments pour vos amis, collègues et relations professionnelles.

Ces guides, bien que plutôt complexes, présentent des instructions sur comment mettre en place PGP avec votre mail. N'importe quelle adresse mail peut être utilisée avec un chiffrement PGP !

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

#INTRODUCTION

#ANONYMAT

#HACKING

#DATA

#TÉLÉPHONES

#CHEAT SHEET