Protégez vos comptes en ligne

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 protéger mes comptes en ligne. Je sais que des arnaques sont courantes mais rien n'y fait, je continue de garder le même mot de passe depuis mon premier compte Caramail... 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.

#HACKING

Vos comptes sont des points d'accès à votre vie en ligne et hors ligne. Vos mails, vos réseaux sociaux, votre shopping, vous en avez pour presque tout ce que vous faites sur internet. À l'intérieur de ceux-ci se trouve un trésor de données personnelles, d'informations bancaires et même la possibilité pour quelqu'un d'être « vous ». Malheureusement, les hackers et les agresseurs connaissent la valeur d'avoir accès à de tels comptes, cibles principales pour le cyber-harcèlement et le cyber-crime. Cette section offre un certain nombre de méthodes pour rendre le hacking beaucoup plus difficile. **Comme pour tout service numérique, il n'y a pas de méthode infaillible pour vous protéger contre un hacker déterminé (et vous ne devriez jamais faire confiance à quelqu'un qui prétend le contraire)**, mais ajouter des couches de

sécurité vous donne plus de contrôle sur votre identité et vos informations en ligne, ce qui peut dissuader ou prévenir des formes communes de hacking.

Alors que nous esquissons les meilleures pratiques à avoir, les technologies les plus utiles à installer et vous recommandons certains services, il est fondamental d'être conscient-e des risques liés à chaque contexte. La meilleure chose à se demander est : « Si c'était hacké, quel impact ça aurait sur ma vie ? » Envisager les choses sous cet angle signifie que VOUS pouvez dicter la sécurité et la privacité de votre vie numérique. Vous pouvez choisir d'ajouter plus de mesures, ou moins. Vous pouvez choisir d'utiliser un service plus sûr, ou rester avec ce que vous avez. C'est à vous de décider !

Ingénierie sociale et hameçonnage

Croyez-le ou non, la majorité des succès de hacking ne requièrent pas des compétences très avancées. Des espions gouvernementaux aux trolls pathétiques, les hackers malveillants dépendent généralement de combines simples pour piéger les gens afin qu'ils donnent leurs mots de passe, mails ou autre informations privées. **L'ingénierie sociale implique une manipulation psychologique des cibles pour révéler des informations sensibles.** Un exemple courant est un appel d'un hacker à un service client ou service technique sur un site internet : il prétend être un employé ou un client et après avoir lancé la conversation il arrive à obtenir des informations sur un autre client. Un autre cas courant est de simplement contacter la cible et de se faire passer pour un représentant de la compagnie : un hacker peut prétendre être un employé d'un fournisseur quelconque nécessitant une information sur votre appartement, ou un employé d'assurance pour connaître votre plan de santé, ou incarner n'importe quel rôle pour vous voler des informations. **Le hameçonnage est une forme très populaire de l'ingénierie sociale, où un hacker vous enverra un mail qui aura l'air professionnel prétendant être un site ou un service, en incluant un lien à suivre.** Lorsque vous cliquez dessus, il vous emmènera vers un site qui semblera légitime qui vous demandera votre passeport, votre code pin ou n'importe quelle autre information. Mais en réalité, le site est un faux qui recueille les données privées que vous donnez par erreur !

Alors, comment vous protéger contre ces sortes d'attaques ? Voici quelques repères qui pourront vous aider !

Ne vous connectez pas à un site à partir d'un lien dans un mail

En règle générale, si un lien dans un mail vous dirige directement à un écran de connexion, vous devriez être suspicieux-se. Il vaut mieux vous rendre sur le site vous-même à partir de votre navigateur, vous connecter normalement et chercher la page proposée dans le mail. Une exception, quand vous devez mettre à jour votre mot de passe sur un site (celui-ci a besoin de vous fournir un lien personnalisé pour que vous puissiez le changer). Dans ce cas, c'est juste pour s'assurer que vous avez effectivement fait la demande. Et utilisez un mot de passe unique, juste pour être sûr-e !

Toujours installer les mises à jour de logiciel le plus vite possible

Les hackers dépendent souvent des vulnérabilités exploitables dans les logiciels populaires pour cibler leurs victimes. Les développeurs peuvent rapidement devenir conscients de ces vulnérabilités et sortent des mises à jour pour régler le problème. Il est impératif que vous gardiez un logiciel à jour pour que vos applications aient les dernières corrections de sécurité ! C'est très simple à faire : quand votre ordinateur vous notifie qu'il y a des mises à jour à installer, allez-y et faites-le. Assurez-vous surtout d'installer les mises à jour des systèmes d'exploitation macOS, iOS, Android et Windows le plus vite possible !

Essayez de ne pas vous connecter aux sites via Facebook, Twitter ou Google

De nombreux sites offrent la possibilité de vous connecter grâce à votre compte de réseau social plutôt que d'avoir à en créer un nouveau. Bien que pratique, cela représente un énorme risque de sécurité : comment savez-vous si ce site est légitime ? En encourageant des utilisateurs peu méfiants à utiliser leur compte de réseau social, un site malveillant peut facilement recueillir des noms ou mots de passe. Il est beaucoup plus sûr de se créer un nouveau compte pour le site.

Ne vous fiez pas aux mails vous demandant des informations professionnelles, des données statistiques ou n'importe quelle autre information à propos de vous, peu importe s'ils paraissent pro

La majorité des sites n'ont pas besoin de vos données personnelles pour vous fournir un service, donc soyez suspicieux-se si on vous les demande (en plus, on s'en fout de ce qu'ils veulent, non ? Ce n'est pas votre responsabilité de leur donner *quoi que ce soit*). Si vous pensez que la requête est légitime, ne suivez pas le lien fourni : vous devriez pouvoir faire ce que vous voulez en allant sur leur site à partir de votre navigateur. Si vous ne pouvez pas, ils ont clairement des pratiques de sécurité de merde et vous devriez vous méfier d'eux de façon générale !

Utilisez des connexions HTTPS à chaque fois que c'est possible

Dans la section sur l'anonymat, nous avons parlé de l'avantage d'utiliser l'extension HTTPS Everywhere. Quand vous vous connectez à un site en utilisant HTTPS, votre navigateur s'assure que le site n'est pas un faux en vérifiant si son certificat HTTPS est légitime. Parce que des faux sites ne peuvent pas reproduire le certificat attendu, votre navigateur peut vous prévenir que ce site pas sûr. **Faites confiance à votre navigateur !** En installant l'extension HTTPS everywhere, votre navigateur va tenter d'utiliser HTTPS le plus possible, offrant donc une première ligne de défense facile contre les combines d'hameçonnage.

Méfiez-vous du wifi public

Quand vous vous connectez au wifi, n'importe qui utilisant ce réseau peut observer ou intercepter votre trafic sur le web (même si c'est un réseau protégé par un mot de passe). Une

combine très simple d'hameçonnage peut très bien vous attendre dans un café, intercepter toutes vos requêtes à facebook.com, envoyer tout le monde sur un faux site à la place et donc récupérer tous les mots de passe. La meilleure des protections est d'utiliser un Réseau Virtuel Privé (VPN) pour chiffrer votre trafic et le rendre impossible à intercepter. Utiliser Tor peut être une très bonne alternative : vous êtes anonyme grâce au chiffrement de vos données (bien que ce sera plus lent qu'un navigateur habituel). Si vous êtes sur votre téléphone, essayez d'utiliser les applications que vous avez installées pour accéder aux sites souhaités plutôt que de vous connecter via un navigateur (les navigateurs sur téléphone sont en effet beaucoup moins sécurisés).

Au final, est-ce que vous devez *vraiment* céder vos informations personnelles ? (… Non)

Assez régulièrement, un site ou un fournisseur de services vous demanderont plus qu'un mail et un mot de passe : ils voudront votre nom, votre localisation et autres données à forte valeur commerciale. Eh bien, qu'ils aillent se faire foutre ! Qui a dit que vous deviez leur dire la vérité ? **Une bonne règle générale est de ne donner vos informations personnelles que dans le cas où c'est absolument nécessaire.** N'ayez pas peur d'inventer ! Vous pouvez toujours donner un faux nom, une fausse adresse et toutes sortes de fausses informations. Sauf si vous achetez quelque chose, toutes ces informations personnelles sont rarement fondamentales. En donnant de fausses données, vous diminuez les risques de lier un compte compromis à d'autres comptes via les données partagées, mais vous réduisez aussi la possibilité pour une personne malveillante d'en savoir plus sur votre vraie vie.

(*Au fait, les adresses mail n'ont pas besoin d'être vraies non plus. Si vous vous enregistrez juste rapidement pour utiliser un site une ou deux fois, utilisez une adresse mail jetable ! C'est particulièrement pratique si vous devez faire quelque chose en ligne sous anonymat. On aime bien utiliser* Sharklasers.com *parce que les requins sont cool mais il y a de nombreux autres*

services identiques sur le web.)

Mots de passe forts : « Ugh »

Pour citer xkcd : « Après 20 ans d'effort, nous avons réussi à entraîner tout le monde à utiliser des mots de passe difficiles pour les humains à retenir, mais simples pour les ordinateurs à deviner. »

On peut accéder à la grande majorité des comptes en ligne grâce à un mot de passe et un mail/identifiant. Comme on le sait tous, un bon mot de passe est essentiel pour s'assurer que les hackers n'aient pas accès à nos affaires. Cependant, la façon dont on les crée et dont on s'en souvient tend à être très facile à hacker : des noms communs ou des phrases peuvent être exploitées par la programmation quand on tente d'accéder à un compte. Comme étant la première et souvent la seule ligne de défense contre l'accès à votre compte, les mots de passe forts sont la clé !

Voici quelques règles générales à suivre pour créer de bons mots de passe forts :

1. Le mieux : un mixe de lettres, nombres et caractères spéciaux au hasard.
2. Plus c'est long, plus c'est bon. 12 caractères ou plus !
3. NE RÉUTILISEZ PAS LE MÊME MOT DE PASSE SUR PLUSIEURS SITES
4. NE RÉUTILISEZ PAS LE MÊME MOT DE PASSE SUR PLUSIEURS SITES

Se souvenir de mots de passe qui suivent ces règles peut se révéler vraiment pénible, surtout quand vous en avez autant. Par chance, xkcd a une approche formidable : **quand vous créez vos mots de passe, prenez une phrase secrète de trois ou quatre mots au hasard**. Ces mots de passe seront non seulement plus faciles à se souvenir, ils sont aussi beaucoup plus difficiles à hacker parce qu'ils sont vraiment longs ! Voici quelques exemples :

1. correcthorsebatterystaple
2. sillyredkitchenplant
3. librarypantherseatvanilla

Gestionnaires de mots de passe : « Cool ! »

Comme vous pouvez vous en douter, faire des mots de passe forts, c'est chiant. Quand vous avez une douzaine de comptes répartis sur plusieurs sites différents, c'est pratiquement impossible d'être parfait en créant et en se souvenant de tous ces mots de passe uniques. Sans parler du fait que certains sites sont horribles quand il s'agit de les stocker : s'ils sont hackés c'est *vous* qui devez changer votre mot de passe. Il existe des outils pour vous aider ! Un gestionnaire est un service en ligne qui peut générer et stocker tous vos mots de passe pour que vous n'ayez pas à les connaître par cœur.

Lifehacker a un guide très pratique qui détaille les gestionnaires les plus populaires.

Vous êtes probablement suspicieux-se : est-ce que ce n'est pas dangereux d'avoir tous vos mots de passe en un seul endroit ? Et vous avez raison, parce que ça l'est ! C'est pourquoi il est important d'évaluer comment tel gestionnaire gère effectivement les mots de passe et quelles protections sont mises en place. Au final, vous devez décider vous-même l'équilibre entre les risques d'un mauvais mot de passe, utilisé par tous vos comptes, contre le risque de bons mots de passe centralisés au même endroit.

LastPass

Étant donné la difficulté de se souvenir de mots de passe sécurisés et uniques, nous vous recommandons quand même d'utiliser un gestionnaire, en particulier **LastPass**.

Lastpass utilise une combinaison d'extensions de navigateurs, d'applications de téléphone, de chiffrement, de double authentification et une multitude d'autres technologies pour assurer que vos mots de passe sont stockés de façon sécurisée et accessible (seulement pour vous!). Il peut aussi générer des mots de passe – extrêmement – forts au hasard. Nous apprécions particulièrement LastPass parce que tous nos mots de passe sont chiffrés lorsqu'ils sont sauvés sur son cloud : même s'ils sont hackés, un hacker ne pourra pas les utiliser sauf s'il connaît votre mot de passe pour LastPass (qui ne sera jamais stocké par LastPass). Inutile de préciser que si vous décidez de l'utiliser, vous devez vous assurer que votre mot de passe d'accès à LastPass est le mot de passe le plus fort que vous ayez jamais eu ! Vous n'aurez plus à vous souvenir des autres, donc ça devrait être un peu plus facile à faire.

Vous pouvez commencer avec LastPass avec leur site officiel.

Tant qu'on parle de diminuer les risques, nous vous recommandons de ne pas utiliser LastPass pour votre mail, votre banque ou les services de santé en ligne. Bien que LastPass soit un service très sécurisé, ça reste une compagnie sujette à des erreurs et des vulnérabilités. En séparant vos mots de passe cruciaux, vous avez une petite protection en plus en n'ayant pas TOUS les œufs dans le même panier. Les œufs les plus importants méritent d'être gardés dans votre propre panier !

Quelques bonnes règles générales d'utilisation pour LastPass :

- Utilisez un générateur pour des mots de passe longs et compliqués. Le mieux : au moins 16 caractères avec des lettres, nombres et symboles.
- Assurez-vous d'activer l'authentification double pour LastPass.
- Toujours demander un mot de passe principal pour accéder aux mots de passe de vos comptes importants.
- Une fois que vous vous êtes enregistré-e à LastPass depuis votre téléphone et/ou tablette, allez sur le site de LastPass, dans Settings, sous l'onglet « Mobile Devices », assurez-vous d'avoir coché « Restrict mobile devices to the specific UUIDs listed as enabled below ». De cette façon, seuls les appareils spécifiés peuvent être utilisés pour vous connecter à votre compte LastPass.

Double authentification : « Yay ! »

L'une des meilleures choses que vous pouvez faire pour vos comptes en ligne est d'activer la double authentification (2FA) à chaque fois que c'est possible. En gros, au lieu de n'avoir besoin que d'un mot de passe, vous devrez entrer un deuxième morceau de données. C'est typiquement un court code envoyé dans un mail, un sms ou généré par une application sur votre téléphone. 2FA est un outil fantastique de sécurité parce que ça signifie que même si vos mots de passe sont hackés, un hacker doit aussi avoir accès à votre mail, votre téléphone ou l'application pour pouvoir accéder à vos comptes.

Vous devriez définitivement activer 2FA pour tous vos comptes cruciaux qui le proposent. La plupart des grosses machines comme Google, Facebook, Dropbox et Twitter ont une option disponible, comme pour les gestionnaires de mots de passe populaires comme LastPass. En gros vous devez chercher dans les paramètres des comptes liés aux sites pour trouver comment l'activer. Voici un guide pratique de Google si vous voulez en savoir plus sur le fonctionnement de l'authentification à double facteurs.

Authy

Quand vous utilisez un site ou un service qui propose la double authentification (2FA), vous avez souvent l'option pour générer un QR code ou un code numérique que vous rentrez ensuite dans une application 2FA sur votre téléphone. À partir de là, quand vous vous connectez à un site ou un service qui peut supporter un code 2FA, vous avez juste à regarder dans l'application pour un code généré à utiliser sur ce compte. C'est plus sécurisé que de recevoir un code par sms ou mail, mais aussi plus difficile pour un hacker ou une surveillance d'y avoir accès. Bien qu'il y ait de nombreuses applications qui offrent cette fonctionnalité, nous recommandons Authy.

Authy est une super application qui génère automatiquement vos codes de double authentification hors ligne, partout où vous l'avez installée. Authy peut être installée sur votre téléphone ou votre bureau, avec tous vos comptes générant des codes 2FA, le tout sur un seul compte. Cela signifie que si vous perdez votre téléphone, ou si vous achetez un nouvel ordinateur, tout ce que vous avez à faire est d'installer Authy et de vous connecter (ayez un mot de passe très fort!!) et vos codes 2FA seront à nouveau générés sans problème. Vos comptes 2FA sont aussi chiffrés dans le cloud, c'est-à-dire que si les serveurs de Authy sont hackés, vos données seront inutilisables ! Et parce que ces codes sont générés hors ligne, vous n'avez pas besoin d'avoir internet ou avoir recours à un service téléphonique pour y avoir accès.

Disponible gratuitement sur iTunes ou Google Play, Authy a aussi une extension chrome

Les guides d'installation peuvent être trouvés sur le site d'Authy

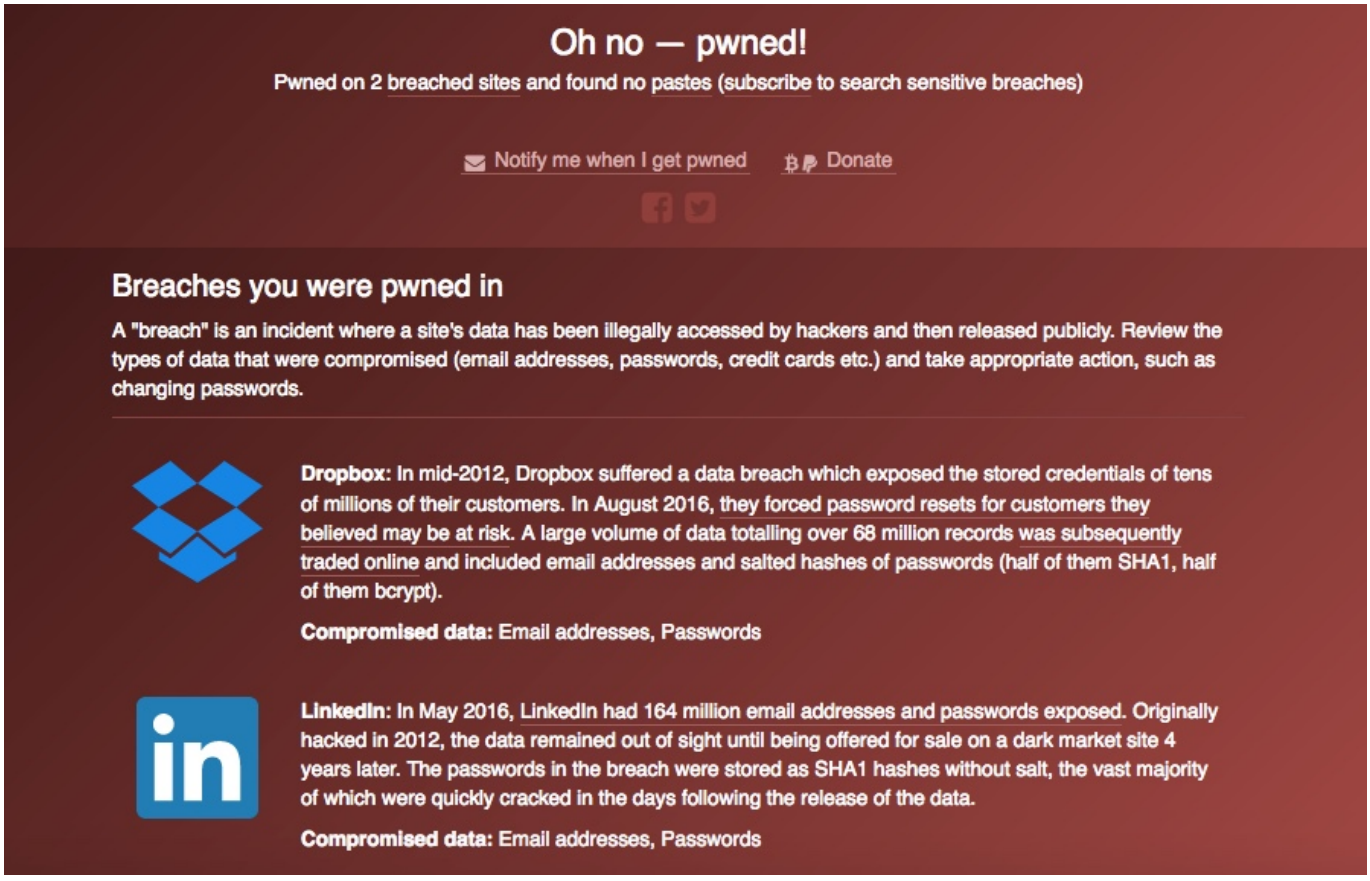
Alors… comment je sais que j'ai été hacké-e ?

Les compagnies privées ont certaines des pires pratiques de sécurité imaginables. Vos mots de

passe peuvent être stockés dans leurs bases de données en clair, associés à votre mail ou votre répertoire de mails, parfois même avec vos informations bancaires. **Il n'existe aucune législation obligeant les compagnies à prendre votre sécurité au sérieux, du coup très peu d'entre elles le font. En conséquence, les hacks de compagnies et les fuites deviennent de plus en plus courants et continueront d'être fréquents tant que le big data exploite et vend d'énormes quantités de données personnelles.** Vous avez probablement entendu parler de ces hacks aux infos, mais ils font rarement des vagues et sont vite oubliés. Malheureusement, ces données privées ne disparaissent pas avec le temps : elles sont agrégées à travers internet et stockées indéfiniment, parfois par des hackers, ou parfois par des professionnels de la sécurité. Donc, si vous n'êtes pas au courant qu'une compagnie fait fuiter vos données, ou vous avez simplement oublié, vous pouvez très bien être une cible (ils ont vos données personnelles, après tout).

Allez sur haveibeenpwned pour voir si votre mail ou votre identifiant a déjà été compromis dans une faille majeure de données. Votre seule action de défense possible est d'utiliser des **mots de passe forts et uniques** et la **double authentification** pour tous vos comptes importants.

Si une ni deux, j'ai testé mes mails et identifiants sur le site haveibeenpwned : manque de bol, j'étais compromise.



J'ai évidemment immédiatement changé mes mots de passe... Tout en essayant de me remémorer ce que j'avais sur Dropbox au moment des faits. Rien de compromettant, sûrement. J'avais toujours fait attention à ne pas partager de documents sensibles ou d'informations sur mes sources, sachant le service peu fiable. Il était de toute façon trop tard pour ce qui avait fuité. Mes réflexes sont de plus en plus affinés : je n'ouvre jamais une pièce jointe dont je ne connais pas le destinataire, je vérifie toujours que je suis sur une page https:// avant de me connecter à un site et j'ai modifié tous mes mots de passe en les rallongeant et en y ajoutant toutes sortes de chiffres et de lettres. Ce que je n'ai pas encore résolu, par contre, c'est la tentation de me connecter à des sites directement avec mon compte Facebook... C'est si facile...

#INTRODUCTION

#ANONYMAT

#DATA

#TÉLÉPHONES

#SOCIAL

#CHEAT SHEET