Ce que vous devez savoir et faire pour protéger vos données.

La sécurité de vos données sur internet est primordiale et c'est un sujet d'actualité ! Piratage de votre compte e-mail, de vos profils sur les réseaux sociaux, de votre compte bancaire en ligne et même de votre site Jimdo... Il est très important d'observer quelques règles de sécurité afin de se protéger au mieux des risques de piratage et de préserver ses données privées. Nous vous en présentons 5 :

Utiliser des mots de passe de qualité

Une équipe d'ingénieurs spécialisée dans la sécurité a récemment découvert un bug dans l'un des protocoles de cryptage les plus courants, utilisé par pratiquement tous les sites web qui possèdent des comptes utilisateurs. Ce bug, connu sous le nom de "Heartbleed", provient d'une faille dans la bibliothèque du logiciel OpenSSL. Jargon technique me direz-vous, mais l'important à retenir est qu'il est depuis lors impératif de changer vos mots de passe !

- **Changer de mot de passe régulièrement**

Plus les données à protéger sont importantes, plus vos changements de mot de passe doivent être fréquents. Une fois tous les 3 mois minimum !

- **Comment choisir votre nouveau mot de passe ?**

Un mot de passe "fort" est avant tout un mot de passe long. Nous vous recommandons d'utiliser au minimum 8 caractères.
La tendance actuelle en matière de sécurité consiste même à utiliser une "phrase de passe". (Comprenez ici l'utilisation d'une phrase plutôt que d'un mot.)
En effet, même sans utiliser un grand nombre de caractères spéciaux, une phrase sera plus dure à décrypter par les pirates qu'un mot. Pour encore plus de sécurité, utilisez une phrase qui associe majuscules, caractères spéciaux et chiffres !

Exemple :
"ViveJimd0CestSuperSimple!"
sera plus sur que :
"J@845Rt" .

- **Ne jamais utiliser le même mot de passe pour plusieurs comptes !**

D'accord, mais un bon de mot de passe est souvent difficile à retenir ! Dans ce cas, nous vous recommandons d'utiliser une « routine » : choisissez une structure qui se répète et dont seulement une partie change pour chaque mot de passe que vous créez.

Une routine classique :
Commencez avec la première lettre ou la syllabe du site pour lequel vous créez ce mot de passe (différent pour chaque compte donc) + la première phrase de votre chanson préférée (toujours la même) + une date importante pour vous et finissez par la dernière lettre ou syllabe du site pour lequel vous créez ce mot de passe.
(Attention : ceci est un exemple, inventez une routine bien à vous !)

Exemple :
Votre chanson préférée est "Amsterdam" de Brel, la date importante est 1515.
Votre phrase de passe pour votre site Jimdo sera :
JimDansleportd'Amsterdam1515Do

- **Ne jamais laisser votre navigateur mémoriser vos mots de passe.**

Cette pratique vous fait peut-être gagner du temps mais vous courrez le risque que quelqu'un de mal intentionné se connecte à l'un de vos comptes sans même avoir à saisir un mot de passe, en accédant à votre ordinateur, votre tablette ou votre mobile.
Idem, ne laissez pas en vue un post-it avec tous vos identifiants sur votre bureau !

Mettre à jour ses logiciels : navigateur, antivirus, pare-feu personnel

La plupart des pirates internet tentent d'utiliser les failles du système d'exploitation ou des logiciels pour entrer dans votre ordinateur et avoir ainsi accès à vos données. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger ces failles. Et opter pour un anti-virus de qualité !**Bitfender**, **Avast** et **McAfee** sont des exemples de logiciels recommandés.

Effectuer des sauvegardes régulières de vos données

Pour être sur que vos données sont en sécurité, rien ne vaut une sauvegarde régulière : copiez vos données et transférez-les sur un autre support que le disque dur de votre ordinateur.
Cet autre support peut alors être un disque dur externe ou un service de sauvegarde en ligne. (Choisissez un service reconnu et sérieux : Dropbox ouGoogle Drive peuvent être des solutions intéréssantes).
Il est important d'adapter les solutions de sauvegarde à vos besoins (en particulier si vous êtes une entreprise !). La perte ou le vol de vos données peut avoir des conséquences dramatiques.

Sauvegardez vos données sur :
- Un disque dur externe (privilégiez la technologie SSD)
- Time machine (sur mac OS seulement)
- Google Drive
- Dropbox

Ne pas suivre n'importe quel lien

Une autre attaque classique sur internet consiste à tromper l'internaute lorsqu'il surfe de site en site, en l'incitant à cliquer sur des liens qui ne mènent pas là où ils l'annoncent. Ces liens trompeurs poursuivent souvent des objectifs malveillants. Si vous avez un doute sur le contenu d'un site, avant de cliquer sur un lien proposé par ses pages, passez simplement la souris sur le lien en question pour voir la nature de ce dernier ou ouvrez celui-ci en saisissant directement l'adresse url dans la barre de votre navigateur. Vous éviterez ainsi les trackers qui visent à vous suivre lors de vos futures navigations en espérant obtenir au passage des informations personnelles pour ensuite les livrer à des personnes malveillantes.

Ne jamais ouvrir un e-mail sans réfléchir

N'ayez pas une confiance aveugle dans les e-mails que vous recevez, même s'ils proviennent d'un expéditeur connu ! Votre activité et celle de ceux avec qui vous communiquez sur internet peuvent malheureusement permettre à des personnes malveillantes de récupérer votre adresse e-mail. Ce n'est pas directement dangereux en soi, mais celles-ci essaieront ensuite de vous soutirer informations ou argent en vous envoyant des e-mails trompeurs, et en se faisant passer pour ce qu'ils ne sont pas. Alors prudence, ne répondez jamais à une demande d'information confidentielle par e-mail et méfiez vous également des pièces jointes. Elles peuvent contenir des virus ou des logiciels espions

Collé à partir de <http://fr.jimdo.com/2014/07/01/les-5-r%C3%A8gles-de-base-de-s%C3%A9curit%C3%A9-sur-internet/?utm_source=Newsletter+%5Bfr_FR%5D&utm_campaign=47c2007bdd-2014_07_31_NL_FR_Juillet&utm_medium=email&utm_term=0_bb5660a135-47c2007bdd-129440297>