Dix règles pour vous prémunir contre le piratage de vos données personnelles

Par Bercy Infos, le 10/10/2022 - Droits et protection sur internet

Vous pensez être anonyme sur le web ? Que personne ne trouvera votre mot de passe ? Que votre code wifi vous protège amplement ? Faux ! Si vous souhaitez vous protéger contre les risque de piratage de vos données, voici quelques conseils à suivre !

1. Créez des mots de passe sécurisés

Utilisez des mots de passe de qualité, sans quoi vous risquez de faciliter l'accès à vos données personnelles. Privilégiez les **mots de passe longs**, comprenant des majuscules et des minuscules, des chiffres, et des caractères spéciaux. Par exemple : Wejd*25ipO%Ram.

Nombre de pirates disposent en effet de logiciels leur permettant de générer toutes les combinaisons du dictionnaire, voire des formules plus complexes. Des mots de passe tels que « chocolat », votre date d'anniversaire ou le nom de votre mascotte sont donc à proscrire.

C**hangez votre mot de passe régulièrement** et choisissez-en un **différent pour chacun de vos comptes**. En effet, une fois qu'un hacker (cyberpirate) a trouvé l'un de vos mots de passes, il va essayer d'accéder à vos autres comptes avec celui-ci. Si vous avez reçu un nouveau mot de passe par courriel, n'oubliez pas de vous débarrasser de ce message.

À savoir
Vous souhaitez en savoir plus sur la sécurisation de vos mots de passe ?

Consultez les conseils de l'Agence nationale de la sécurité des systèmes d'information (ANSI).

2. Mettez votre système d'exploitation à jour

Votre système d'exploitation (navigateur, antivirus, bureautique, pare-feu personnel, etc.) doit être à jour.

Les agresseurs profitent en effet des logiciels non mis à jour afin d'utiliser les failles non corrigées par votre système pour s'y introduire. C'est la raison pour laquelle la mise à jour de vos outils est essentielle.

3. Portez attention à votre clé wifi !

Il existe plusieurs types de clés wifi. La clé WEP est la plus courante, car elle reste habituellement le choix par défaut des fournisseurs d'accès. Mais c'est également la moins sécurisée. Les clés WEP peuvent être décryptées par des pirates en quelques minutes, contre une quinzaine d'heures pour une **clé WPA 2**.

Pour basculer vers cette dernière, saisissez « 192.168.1.1 » sur la barre d'adresses de votre navigateur internet ou accédez directement aux paramètres de votre wifi depuis votre compte personnel en ligne auprès de votre fournisseur d'accès.

4. Sauvegardez vos données

Ce conseil ne vous protègera pas d'une attaque malveillante mais pourra au moins en réduire les conséquence. En effet, l'une des meilleures façons de se prémunir contre les pertes de données suite à une attaque, est tout simplement de les **sauvegarder assez régulièrement**.

Vous pourrez ainsi retrouver vos fichiers si vous ne parvenez plus à y accéder sur votre ordinateur. Un disque dur externe ou une clé USB (que vous débrancherez une fois l'opération de sauvegarde terminée) feront très bien l'affaire.

5. Méfiez-vous des liens

Ne cliquez pas trop vite sur les liens, même ceux qui vous paraissent familiers. Une des attaques les plus classiques vise à tromper l'internaute en l'incitant à cliquer sur des liens figurant dans un e-mail ou une page web. Ce lien peut-être malveillant.

En cas de doute, **abstenez-vous et préférez écrire vous-même l'adresse voulue dans la barre d'adresses** de votre navigateur.

6. Soyez vigilant concernant les pièces jointes dans les courriels

Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles peuvent contenir des codes malveillants. Faites particulièrement attention à celles dont les extensions se terminent par .pif ; .com ; .bat ; .exe ; .vbs ; .lnk : recevez-vous ce type de pièces jointes habituellement ? Par exemple : photosvacances.pif

7. Ne naviguez pas sur le web depuis votre compte administrateur

L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur.

Préférez l'utilisation d'un compte utilisateur, qui vous permet également de naviguer sur le web sans entraves.

8. Soyez attentif à ce que vous écrivez sur le web !

Il est très important de contrôler la diffusion d'informations personnelles.

Internet est loin d'être ce lieu d'anonymat qu'on imagine. **Évitez de fournir vos coordonnées ou d'autres données sensibles** dans les forums, sur des sites n'offrant pas toutes les garanties requises ou même sur les réseaux sociaux.

Un conseil : le symbole ***https://*** au début de l'adresse web et l'image d'un petit cadenas est gage de site web certifié et sécurisé, mais dans le doute, mieux vaut s'abstenir.

9. Utilisez un antivirus ou un pare-feu

Aucun ordinateur n'est imprenable, mais ne facilitez pas la tâche aux hackers.

Mieux vous serez protégé, plus rude et dissuasive sera la tâche pour les personnes malveillantes.

En informatique, le pare-feu permet de limiter un certain nombre de connexions entrantes et sortantes. Si malgré tout, le pirate trouve une faille dans votre ordinateur, un antivirus peut l'empêcher de nuire.

10. Méfiez vous de tous les expéditeurs, même ceux que vous connaissez

L'envoi de liens malveillants peut-être indépendant de la volonté de leurs expéditeurs, même de ceux que vous connaissez !

Si un correspondant avec lequel vous échangez régulièrement vous adresse par exemple un message dans une langue étrangère, ou que sa manière de s'exprimer est différente, **n'ouvrez pas les pièces jointes** contenues dans son message et ne cliquez pas sur les liens qui y figurent. En cas de doute, passez-lui un coup de fil !