Un mot de passe pour protéger vos données Internet.

Je reçois de plus en plus souvent un mail avec l'appel à l'aide d'un ami en voyage qui me demande de le contacter uniquement par e-mail… Bref, un vieux truc que des escrocs ont mis en place pour soutirer de l'argent. Ils ont réussi à pirater la boite mail de l'ami en question et envoient ce message à tous ses contacts.

> **Un exemple de mail "sympa":**
> Bonjour, j'espère que tu recevras bien mon mail. Comment vas-tu ce matin ?
> De mon côté, ce n'est pas vraiment agréable...
> Pouvons-nous échanger par mail en toute Confidentialité ?
> J'ai une situation assez importante à t'expliquer, c'est tellement délicat.
> PS: Je tiens à te dire que mon tél est hors service.

Le premier conseil est de ne pas répondre à ce type de mail et de le supprimer sans état d'âme. Si un ami est dans le besoin, il trouvera bien un autre moyen pour qu'on puisse le joindre.

Le second est de protéger l'accès à vos données Internet pour éviter que vous ne deveniez à votre tour l'ami voyageur. Votre porte d'entrée est équipée d'une serrure de sécurité. Ce doit être la même chose pour votre internet : un mot de passe robuste doit empêcher une personne malveillante de le pirater.

Quelques conseils donnés par un organisme gouvernemental, l'ANSSI, peuvent vous aider à améliorer la qualité des « serrures » de votre fournisseur d'accès, de votre messagerie, de votre banque. C'est le minimum à protéger.

- N'utilisez pas le même mot de passe pour tout votre Internet. C'est pratique pour vous, mais surtout pour votre pirate !
- Un mot de passe doit être composé d'au moins 12 caractères et être complexe. Il doit comprendre des lettres majuscules, des minuscules, des chiffres ET des caractères spéciaux (&=+-*/ ?;:!...). Ils seront ainsi difficiles à trouver à l'aide d'outils automatisés.
- Le mot de passe ne doit pas avoir de lien avec vous (date de naissance, loisir, nom du chien…).
- Ne stockez pas vos mots de passe dans un fichier de votre ordinateur, mais plutôt sur un carnet.
- Si un logiciel vous demande s'il faut enregistrer le mot de passe, la réponse doit être NON.

Tout ça c'est bien gentil me direz vous, mais comment construire un **mot de passe efficace** ?

Choisir une phrase facile à retenir, voici deux méthodes assez souvent utilisées :

- La méthode phonétique : « *J'ai acheté huit cd pour cent euros cet après-midi* » deviendra **ght8CD%E7am** ;
- La méthode des premières lettres : la citation « *un tien vaut mieux que deux tu l'auras* » donnera **1tvmQ2tl'A.**

Je vous déconseille bien sûr d'utiliser ces 2 mots de passe.

On peut aller beaucoup plus loin dans la protection des données, mais si vous appliquez déjà ces conseils, j'aurai beaucoup moins d'amis à ne contacter que par mail.

Soyez prudent lorsqu'il faut cliquer sur un lien. Si le lien vous est envoyé par une connaissance, peu de risque. Mais si c'est un inconnu qui vous l'envoie, direction poubelle.

Soyez méfiant. Votre banque, le Trésor Public, par exemple, ne vous demanderont jamais vos coordonnées bancaires par mail. Mieux vaut un appel téléphonique à l'expéditeur supposé du mail si vous avez un doute.

Ces conseils ne sont pas faits pour vous faire peur au point de ne plus vous servir d'internet, mais pour vous rendre plus prudent. Les voleurs n'aiment pas perdre leur temps. Si c'est trop difficile de pirater cet ordinateur, ils vont y renoncer.

Des liens pour connaitre les bonnes pratiques conseillées par l'ANSSI, https://www.ssi.gouv.fr/entreprise/precautions-elementaires/dix-regles-de-base/

Et pour en savoir plus sur les mots de passe :

https://www.ssi.gouv.fr/guide/mot-de-passe/

Pour les utilisateurs de liaisons Wi-Fi, voici quelques compléments.

Wi-Fi : Les dangers du Wi-Fi gratuit

Très pratiques, placés dans les centres commerciaux, les gares, les aéroports, les cafés, les transports, chez des particuliers (certains opérateurs internet), etc. Ces accès permettent d'éviter d'utiliser son forfait de téléphone mobile.

Ceci concerne autant les smartphones et les tablettes que les ordinateurs.

Ces réseaux ne sont pas sécurisés (pas de cadenas sur le nom de la borne). L'onde radio, et surtout les données qu'elle transporte, peut être surveillée par des personnes malveillantes souhaitant voler vos codes et vos données.

Que faire ?

- Vérifiez que le pare-feu et l'anti-virus sont bien actifs.
- Supprimez les partages de fichiers entre vos machines.
- Demandez au responsable des lieux confirmation du nom du réseau. Il peut y avoir de faux réseaux au nom voisin géré par un pirate pour voler vos codes.
- Quand vous allez sur Internet, préférez les sites dont l'adresse commence par « https ». Un cadenas fermé s'affichera près de l'adresse.
- Si vous n'avez plus besoin du Wi-Fi (et du Bluetooth) arrêtez les.
- Pas de connexion automatique sur ce genre de borne non sécurisée.
- N'allez pas sur des sites très sensibles (banques, e-mail, réseaux sociaux et tous les sites où vous avez des informations confidentielles).
- En cas de besoin, utilisez plutôt le forfait de données de votre mobile.
- Privilégier les bornes Wi-Fi sécurisées dans les hôtels par exemple (demander le code).
- Vérifiez que l'adresse du site que vous consultez correspond à celle attendue.

Si c'est pour consulter la météo, des horaires ou le site de l'office de tourisme, le risque d'utiliser un accès ouvert est limité mais n'y faites pas une réservation.

Voir les informations sur le site de la Commission Nationale Informatique et Liberté :

https://www.cnil.fr/fr/utiliser-un-wifi-public-voici-5-precautions-prendre