

On ne saurait aujourd'hui se passer d'Internet pour s'informer, acheter, communiquer, travailler. Mais quid de la sécurité de nos données personnelles ? Même si la navigation est de plus en plus fiable, il est important de rester prudent. Voici quelques bonnes pratiques pour éviter piratages, virus, et autres déconvenues.

INTERNET: êtes-vous assez prudent ?

Sonia Julaud

Choisir des mots de passe complexes

Saviez-vous qu'aucun mot de passe n'est réellement inviolable ? Le niveau de protection qu'il vous apporte est en fait directement lié au temps que mettrait un hacker à le déchiffrer, grâce à des logiciels qui explorent le nombre de possibilités de codes selon le nombre de caractères du mot de passe. Mais rassurez-vous, si vous choisissez un mot de passe suffisamment compliqué, ce temps de piratage peut aller jusqu'à des siècles ! Alors un bon mot de passe, c'est quoi ?

On oublie bien sûr les 00000, 12345, dates de naissance, prénoms, etc. Beaucoup trop faciles à trouver ! L'idéal est une combinaison (minimum 8 caractères) de lettres et chiffres, incluant des majuscules et des caractères spéciaux (lettres accentuées, parenthèses, symboles).

Partant de là, voici une méthode efficace:

- Choisissez une phrase (des paroles de chansons, le premier vers d'un poème, le titre de votre film préféré, etc.)
par exemple : Le Bonheur Est Dans Le Pré
- Prenez la première lettre de chaque mot : lbedlp
- Ajoutez quelques chiffres et symboles faciles à retenir: l554bedlp&&

Astuce de pro

Incluez des caractères propres à la langue française: ç - é - è - î, etc. Le langage informatique étant l'anglais, votre mot de passe n'en sera que plus difficile à pirater !

Utilisez des mots de passe différents pour chaque site

Mais comment faire pour les retenir ? C'est simple: utilisez la méthode ci-dessus, mais choisissez une phrase en rapport avec le site. Par exemple « *Toute Ma Vie En Photo* » (tmvpe) sur Snapchat, ou encore « *J'Adore Games Of Thrones* » (jagot) sur Netflix.

Refusez systématiquement la mémorisation des mots de passe lorsqu'elle est vous est proposée par votre navigateur Internet.

Savez-vous qu'en entreprise, 84% des incidents de sécurité sont causés par des erreurs ou négligences humaines, et non par des défaillances techniques? Ce chiffre souligne votre rôle dans cette sécurité!

Effacez les cookies de votre ordinateur chaque jour

Pourquoi ? Parce qu'ils stockent des données liées à votre navigation sur Internet, pouvant être ensuite récupérées par des logiciels malveillants. Comment ? En allant dans l'historique de votre navigateur, et en cochant la case « supprimer les cookies ». En 2 secondes, c'est fait !

Communiquez vos données personnelles avec prudence

Prénom, nom, adresse, date de naissance : toutes ces informations peuvent être utilisées pour usurper votre identité. Soyez donc très vigilants lorsque vous devez les communiquer en ligne. Assurez-vous que le site soit sécurisé (l'adresse commence par « https »), officiel et fiable.

Un mail d'EDF, de votre CAF, du service des impôts? Attention!

Nous avons tous reçu des messages annonçant un remboursement, un crédit d'impôt, ou bien la nécessité urgente de confirmer nos données personnelles ou bancaires sous peine de ne plus recevoir de prestations, par exemple. Or, la loi stipule bien que « aucune institution ni aucun opérateur n'est autorisé à demander les coordonnées d'une carte bancaire via internet ». Ces mails sont frauduleux et visent à pirater vos données. En cas de doute, ne répondez pas au mail, ne cliquez pas sur les liens qu'il comporte, et contactez la société ou l'administration en question.



« Salut, c'est Sophie, je suis en Inde, j'ai besoin d'argent »

Une amie vous envoie un mail désespéré, vous demandant de lui faire un virement d'urgence ? Alerte, c'est très certainement un faux ! En cas de doute, contactez-la par téléphone, et si ce n'est pas possible, abstenez-vous ! Une entreprise française a déjà fait faillite à cause de ce genre d'arnaque...

Téléchargez uniquement à partir de sites sécurisés (le kiosque d'Apple, iTunes, etc)

Bien sûr, le téléchargement illégal est à vos risques et périls. Les virus qu'il peut apporter sont de plus en plus malveillants et difficiles à éliminer.



Comment savoir si un site marchand est fiable?

Un site truffé de fautes, mal organisé, mal présenté est douteux. Si toutes les réductions offertes sont les mêmes, c'est mauvais signe (beaucoup de sites de vente de chaussures sont frauduleux). La présence d'une section « Mentions légales » est obligatoire en France, si le site n'en comporte pas, c'est donc qu'il est illégal. Durant la transaction, le site doit absolument être sécurisé (mention https dans l'url).

Sur votre mobile

- Ne désactivez jamais le code PIN et changez celui qui vous est donné par défaut
- Mettez en place un délai de verrouillage automatique
- Ne stockez jamais d'informations confidentielles sur votre téléphone : coordonnées bancaires, codes secrets, codes de cartes, etc.
- Notez le numéro IMEI du téléphone pour le bloquer à distance en cas de vol.

Au cabinet

Protégez l'accès à votre ordinateur.

Activez le verrouillage automatique de l'écran après un certain temps d'inactivité, pour empêcher toute utilisation intempestive par un tiers, surtout si votre ordinateur est situé dans un endroit passant.

Faites des sauvegardes fréquentes

Sur un disque dur externe (que vous conservez sous clé) ou sur un espace de stockage en ligne (dans le « cloud »).