Une bonne protection de base contre la cybercriminalité en cinq étapes

Possédez-vous un smartphone, un ordinateur portable et/ou une tablette ? Vous avez peut-être aussi une smart TV et d'autres appareils qui sont connectés à Internet ? Si c'est le cas, vous savez très certainement à quel point il est important de bien les protéger. Mais savez-vous comment ? Suivez ces cinq étapes essentielles pour surfer sur le web de manière plus sécurisée.

1. Faites preuve de bon sens

Un bon pare-feu ne suffit pas à vous protéger. Vous êtes vous-même la meilleure défense contre les cybercriminels. Un coup de téléphone du soi-disant service technique de Microsoft ? Ou un e-mail vous demandant vos données bancaires ? Ce ne sont que quelques-unes des ruses que les cybercriminels ont imaginées pour avoir accès à votre PC et à vos données confidentielles. Soyez donc toujours sur vos gardes et faites preuve de bon sens !

ASTUCE:

Quelqu'un vous demande vos données bancaires ? Ne donnez jamais vos codes d'accès !

2. Mettez régulièrement vos logiciels à jour

Votre téléphone portable, tablette, ordinateur ou vos applications vous demandent régulièrement de faire des mises à jour. Celles-ci ne sont pas effectuées dans le seul but d'embellir l'appareil ou l'application, de les rendre plus performants ou plus rapides. Elles constituent également pour le fabricant l'opportunité d'éliminer les vulnérabilités au sein de la technologie. En mettant régulièrement

vos appareils à jour, vous rendez la tâche des pirates informatiques un peu plus difficile. Effectuez donc autant de mises à jour que possible pour les appareils connectés à un réseau.

3. Créez un mot de passe fort et unique

Pourquoi ne pas utiliser plusieurs mots accompagnés d'espaces, de symboles et de chiffres comme mot de passe ? Un mot de passe qui est impossible à deviner est plus difficile à pirater par des hackers ou des programmes informatiques. Il est donc très sûr. Veillez aussi à utiliser un mot de passe différent et unique pour chaque compte en ligne, application et appareil.

ASTUCE :

Si possible, mettez en place une authentification en deux étapes ! De cette manière, vous serez encore mieux protégé. Vous ne savez pas comment cela fonctionne ? Facebook, Gmail et d'autres services proposent souvent cette sécurité supplémentaire et vous expliquent en détail ce que vous devez faire pour l'activer pour leurs services.

4. Cryptez vos données

Crypter vos données semble peut-être légèrement tiré par les cheveux, mais cela fonctionne vraiment. Le cryptage est une manière simple et efficace de protéger vos données confidentielles.

Vous pouvez crypter deux types de données :

Les données au repos : données sur votre disque dur et clé USB.
La plupart des systèmes d'exploitation proposent une fonction de cryptage du disque entier. Par ce biais, vous pouvez chiffrer automatiquement vos données au repos.

Les données en mouvement : données qui sont envoyées de votre appareil vers celui de quelqu'un d'autre.
Pour les données en mouvement (comme lorsque vous faites de l'e-banking par exemple), cherchez l'icône du cadenas fermé ou rendez-vous sur une adresse qui commence par "https". Vous êtes ainsi certain que vos données sont en sécurité.

5. Sauvegardes : elles vous “sauvent la vie”

Votre appareil ou votre compte est infecté par un virus ou a été piraté ? Malheureusement, il n'existe qu'une seule façon d'éliminer définitivement tous les programmes malveillants : effacer toutes les données et effectuer une nouvelle installation. Heureusement, vous faites régulièrement des sauvegardes, n'est-ce pas ?

Ne remettez pas à plus tard les sauvegardes. Vérifiez, si possible, que votre appareil fait bien des sauvegardes automatiques. De cette manière, vous ne perdrez jamais vos données importantes et vos photos précieuses.

Source :

https://www.ing.be/fr/my-news/cybercrime?WT.mc_id=email_PRMR160054_Newsletter_May