

5 conseils de base pour votre sécurité en ligne

Une appli ici, un e-mail là. Partager des photos et des vidéos sur les réseaux sociaux. Faire des appels visio avec les amis et la famille. Transférer de l'argent par Tikkie ou l'appli de votre banque. Se connecter sur un site du gouvernement ou le site de votre médecin généraliste par DigiD. Imprimer sans fil, régler l'alarme ou le chauffage chez soi... Internet rend la vie nettement plus agréable et plus simple à beaucoup de personnes.

Il est important que vous protégez bien tous vos appareils et vos comptes. De votre smartphone à votre imprimante, d'Instagram à Gmail. En effet, comme dans le monde physique, des criminels œuvrent malheureusement en ligne. En exécutant ces cinq actions, vous assurerez votre sécurité de base en ligne. Ainsi, vous rendrez la vie nettement plus compliquée aux cybercriminels.

01 - Veillez à disposer de mots de passe sûrs pour tous vos appareils et comptes. Voici les règles à appliquer :

- Plus le mot de passe est long, mieux c'est. Utilisez une phrase secrète.
- Utilisez un mot de passe différent pour chaque compte. Et conservez vos mots de passe dans un gestionnaire de mots de passe.
- Lorsque c'est possible, connectez-vous en deux étapes.

02 - Mettez toujours immédiatement à jour les logiciels de vos appareils connectés



- Un appareil connecté est un appareil qui est connecté à Internet, comme certaines imprimantes, certains babyphones et certaines sonnettes de portes, mais aussi un aspirateur robot.
- Les mises à jour permettent au fabricant de veiller à la sécurité permanente de vos appareils. Alors ne fermez pas les pop-ups !



03 - Utilisez un scanner antivirus

- Un scanner antivirus vérifie l'absence de toutes sortes de désagréments sur votre appareil, comme des virus, des logiciels et des applis malveillants.



04 - Réalisez des back-up réguliers

- Si vous vous faites pirater, vous pouvez tout perdre. Par conséquent, effectuez une copie de vos fichiers par sécurité.



05 - Vérifier d'abord, cliquer ensuite

- Les cybercriminels envoient de faux liens par e-mail, SMS ou demande de paiement. Ils essaient ainsi de vous convaincre de partager des données ou de transférer de l'argent.

Vous voulez en savoir plus sur la sécurité de base en ligne ? Rendez-vous sur la page veiliginternetten.nl/5-tips-basisveiligheid (en néerlandais)