

Les bonnes pratiques de sécurité numérique

1 - Bien choisir ses mots de passe

Un mot de passe est un outil d'authentification utilisé notamment pour accéder à un équipement numérique et à ses données ou encore pour accéder à des espace en ligne comme l'interface de gestion de compte de notre banque. Pour bien protéger ses informations, il est primordial de choisir des mots de passe difficiles à retrouver (*En savoir plus dans le chapitre "SÉCURISER SON AUTHENTIFICATION"*).



2 - Mettre à jour ses systèmes et logiciels

Dans chaque système d'exploitation* (Android, IOS, MacOS, Linux, Windows, etc ...), logiciels ou applications, des vulnérabilités existent. Une fois découvertes par les éditeurs de système d'exploitation ou de logiciels, elles sont corrigées et sont alors proposées aux utilisateurs par l'intermédiaire des mises à jour de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations de piratage et ceux, encore longtemps après la découverte de ces failles et leur correction.



3 - Sauvegarder régulièrement ses données

Pour veiller à la sécurité de ses données, il est fortement conseillé d'effectuer des sauvegardes régulières (*quotidiennes ou hebdomadaires par exemple*). Cela vous permet alors d'avoir nos données en lieu sûr afin de pouvoir simplement et rapidement les retrouver suite à un dysfonctionnement de notre système d'exploitation ou encore suite à une attaque.



4 - Sécuriser l'accès WiFi de son domicile

Bien que l'utilisation d'un accès filaire à sa box et son ordinateur reste plus sécurisé et plus performant. L'utilisation du Wi-Fi est très pratique pour naviguer sur Internet. Cependant, il ne faut pas oublier qu'un Wi-Fi mal sécurisé peut permettre à des personnes d'intercepter nos données et utiliser la connexion Wi-Fi à notre insu pour réaliser des opérations malintentionnées. Voilà pourquoi il est important au minimum de modifier le code d'accès par défaut à sa box Internet et de définir un mot de passe fort.



5 - Être prudent avec l'utilisation de sa messagerie

Les différents emails et les pièces jointes que vous pouvez recevoir jouent souvent un rôle central dans la réalisation des attaques informatiques. Comme la réception de courriels frauduleux, de pièces jointes piégées, etc.. Voilà pourquoi il faut être extrêmement vigilant lors de l'usage de sa messagerie.



6 - Télécharger ses programmes sur les sites officiels des éditeurs

Si vous téléchargez des logiciels ou des applications sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant pas être mis à jour, qui, le plus souvent, contiennent des virus ou des chevaux de Troie*. Cela peut ainsi permettre à des personnes malveillantes de prendre la main à distance sur votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles ou encore pour lancer des attaques depuis votre machine.



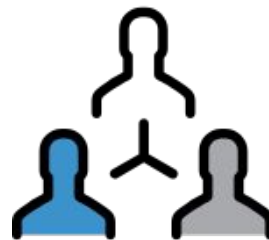
7 - Être vigilant lors d'un paiement sur Internet

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre smartphone, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand. Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet (*présence d'un cadena, mention https présente sur le site en question*).



8 - Séparer les usages personnels des usages professionnels

Les usages et les mesures de sécurité sont différentes sur les équipements de communication personnels et professionnels comme votre ordinateur ou smartphone. Par exemple, il est pertinent de ne pas utiliser son ordinateur professionnel pour réaliser des actions personnelles ou encore laisser cet ordinateur à la portée de ses enfants, qui pourrait sans le vouloir supprimer des données importantes.



9 - Prendre soin de ses informations et de son identité numérique

Les données que nous laissons sur Internet nous échappent instantanément. Comme par exemple lorsque vous spécifiez des informations sur des sites de réseaux-sociaux comme facebook, Twitter ou encore linkedin. Des personnes malveillantes peuvent ainsi utiliser l'ingénierie sociale pour vous piéger. Par exemple ils peuvent avec cette méthode récolter vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, et ainsi accéder à votre ordinateur ou encore votre messagerie. Dans ce contexte, soyez prudent lors de la diffusion d'informations personnelles sur Internet. Suivez notamment les recommandations suivantes pour limiter votre exposition :



- Ne transmettez que les informations strictement nécessaires ;
- Décochez les cases qui autoriserait le site à conserver ou à partager vos données ;
- Ne donnez accès qu'à un minimum d'informations sur les réseaux sociaux ;
- Pensez à régulièrement vérifier vos paramètres de sécurité et de confidentialité ;
- Utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet. Comme par exemple une adresse réservée aux activités dites sérieuses (banques, activité professionnelle...) et une adresse destinée aux autres services (forums, concours, etc...).



Les bonnes pratiques de sécurité numérique

Enfin pour terminer je vous propose de revoir les points développés d'une façon plus décalée avec la vidéo du YouTubeur Micode.

Dans cette vidéo récompensé lors du **Forum International de la Cybersécurité**, Micode nous donne tout ce qu'il faut faire pour être une Cyber-victime ! *(ou tout ce qu'il ne faut pas faire pour éviter d'en être une)*

10 FAUX CONSEILS POUR ÊTRE UNE GROSSE CYBER-VICTIME

