Cyber risques : comment s'en protéger ?

Aujourd'hui, le numérique a pris une place importante dans nos vies : s'informer, faire des démarches administratives, acheter, discuter, etc. Chaque activité en ligne nous expose à de potentiels risques. Voici quelques conseils pour optimiser votre cybersécurité.

Le saviez-vous ? En France*, plus de 9 personnes sur 10 sont internautes chez les plus de 12 ans et 83 % utilisent quotidiennement Internet. Depuis la crise sanitaire, le télétravail et le e-commerce ont connu un essor sans précédent et se sont inscrits durablement dans les pratiques.

Néanmoins, **l'usage d'internet expose à des risques de cybercriminalité ou de piratage informatique**. Parmi les motivations des hackers : vous prendre de l'argent, accéder à vos données, pirater vos réseaux sociaux ou nuire à votre réputation.

Cyber-risque n°1 : attention aux spams dans votre boite mail et SMS !

Qu'est-ce qu'un spam ?

Également appelés "courriels poubelle", ils sont responsables des deux tiers des cas d'infection par des virus, parfois très malveillants : certains peuvent prendre à distance le contrôle de votre terminal, fouiller dans vos données, vos fichiers, pirater vos listes de contacts, vos coordonnées bancaires... Et usurper votre identité pour déjouer la méfiance de vos propres relations sur le net.

À noter : si vous avez identifié un spam, ne répondez pas et ne cliquez pas sur les liens. Bloquez l'expéditeur ou classez-le dans les « indésirables » de votre messagerie.

Il existe plusieurs types de spams et voyons leurs caractéristiques :

Le phishing

Cette technique a pour but de vous « hameçonner », c'est-à-dire de vous convaincre de fournir des informations sensibles ou personnelles, l'émetteur utilisant faussement le nom d'une marque, d'une banque ou d'un assureur...

Ce type de spam invoque souvent un événement vraisemblable : « votre compte bancaire a été bloqué pour des raisons de sécurité. Pour le débloquer, il vous faut cliquer sur un lien »... qui vous amène sur un site, copie plus ou moins conforme d'un site officiel, où l'on vous invite à saisir des informations personnelles : coordonnées bancaires, mots de passe... qui vont faire le bonheur des cybercriminels...

Ne cliquez jamais sur un email qui vous semble douteux

En cas de message écrit en français approximatif, avec une apparence étrange, une adresse mail improbable, ou une adresse connue, mais incohérente avec la demande : dans tous les cas, supprimez immédiatement le message !

Sachez que votre banque, les organismes publics ou les grandes enseignes de distribution ne vous demandent jamais de cliquer sur un lien ou d'ouvrir une pièce jointe, mais de vous connecter de façon sécurisée sur leur site habituel...

Attention :

› L'adresse frauduleuse ressemble vraiment beaucoup à la vraie, il convient donc d'être très attentif !
› Ouvrir les pièces jointes peut vous exposer à des risques de virus et de piratage de vos informations personnelles.
› Limitez la diffusion de votre adresse mail.

Les "rançongiciels"

Ce sont des **logiciels malveillants qui bloquent votre ordinateur et vous demandent de payer une rançon**. Avant de cliquer sur un lien inclus dans un email, vérifiez l'adresse de redirection du site en passant votre souris sur ce lien. Assurez-vous toujours que vous êtes sur le bon site avant de continuer. En cas de doute, fermez votre navigateur.

Cyber-risque n° 2 : les virus informatiques

Première précaution : **installez systématiquement un anti-virus/anti malware** sur vos équipements (smartphone, ordinateurs, tablette, etc.). Il en existe de nombreux, qui proposent soit une version gratuite allégée mais efficace, ou, pour une somme modique, une protection d'excellente qualité.
Vérifiez que vos équipements sont configurés pour faire automatiquement les mises à jour des systèmes et de vos applications.

Autant que possible, **connectez-vous à des sites connus et sécurisés** (la mention « https » se trouve devant l'URL). **Lorsque** vous remplissez des formulaires, ne transmettez que les informations strictement nécessaires.

Soyez sélectifs sur les infos que vous divulguez sur les réseaux sociaux : elles sont potentiellement exploitables par des personnes mal intentionnées. Pour mieux contrôler la diffusion de vos informations, notez que certains moteurs de recherche tel que Qwant, par exemple, ont pour politique de respecter la confidentialité des données sur Internet.

Pour télécharger une application, utilisez uniquement les sites ou magasins officiels (ex : Google Play store, App Store). Méfiez-vous tout spécialement des sites qui proposent gratuitement des applications payantes, ce sont dans la plupart des cas des pièges.

Cyber-risque n°3 : l'usurpation d'identité

Vos mots de passe sont-ils suffisamment sécurisés ? Avez-vous un mot de passe différent pour chacun de vos comptes créés en ligne ? Pour limiter les cyber-risques d'usurpation d'identité par vol de vos identifiants et mots de passe, **utilisez des mots de passe complexes** (plus de 8 caractères, majuscules et minuscules, chiffres et lettre, caractères spéciaux).

Sans cela, vous risquez de perdre le contrôle de vos réseaux sociaux, de votre compte email ou encore de votre compte bancaire en ligne ! Si les doubles vérifications sont de plus en plus proposées lors d'achats en ligne ou pour toute transaction bancaire, restez toujours vigilant.

Cyber-risque n°4 : les clés USB

N'insérez pas une clé USB dont vous ne connaissez pas la provenance. Ces clés sont des vecteurs de choix pour les virus. Veillez à ce que votre anti-virus scanne automatiquement les périphériques que vous connectez à votre PC, et **désactivez la fonction « AutoRun »**, qui lance automatiquement un programme présent sur une clé USB. Une précaution particulièrement nécessaire si vous avez un ordinateur familial, utilisé par vos enfants...

Comment ne pas perdre vos documents personnels ? Faites des sauvegardes

Un disque dur externe ou un abonnement à un service de stockage sur le cloud ("nuage") est une bonne garantie pour conserver vos données, fichiers, photos et films...
Les sauvegardes se font automatiquement, sans intervention de votre part, et les serveurs de stockage font partie des sites les plus sécurisés.
Toutefois, **soyez vigilant dans le choix de la plateforme Cloud que vous souhaitez utiliser afin de stocker des données personnelles.** Privilégiez les services de stockage soumis à la réglementation française et européenne sur la protection des données personnelles.

Vous êtes victime d'une cyber-attaque : que faire ?

Malgré toutes les précautions, un virus malveillant est parvenu à pénétrer vos défenses et à infecter votre ordinateur, votre tablette ou votre smartphone... ? Dès que vous constatez un problème, **déconnectez votre terminal d'Internet**.

Pour ne pas risquer d'aggraver la situation, **confiez alors votre matériel à un professionnel**, qui pourra mettre en œuvre des outils spécifiques pour éliminer la menace, ou, à tout le moins, récupérer l'essentiel de vos données.

Votre compte sur un réseau social a été piraté ? Premier réflexe, rendez-vous sur votre compte pour **modifier votre mot de passe**. Chaque réseau social (Facebook, Twitter, TikTok, etc.) a une **procédure spécifique à suivre** pour une reprise en main rapide de votre espace personnel. Informez vos contacts du piratage pour qu'ils ne cliquent pas sur des liens malveillants envoyés en votre nom.

* **Sources :** Baromètre du numérique – Edition 2021 ; étude CREDOC réalisée pour le compte de l'Arcep, du CGE et de l'ANCT