LES 10 BONNES PRATIQUES À ADOPTER POUR SE PROTÉGER DU RISQUE CYBER

Utiliser des mots de passe de qualité c'est-à-dire difficile à retrouver à l'aide d'outils automatisés, et difficile à deviner par une tierce personne.

Avoir un système d'exploitation et des logiciels à jour : La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels).

Effectuer des sauvegardes régulières. Un des premiers principes de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement.

Désactiver par défaut les composants ActiveX et JavaScript. Les composants ActiveX ou JavaScript permettent des fonctionnalités intéressantes, mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. Il est conseillé de désactiver leur interprétation par défaut et de choisir de ne les activer que lorsque cela est nécessaire et si l'on estime être sur un site de confiance.

Ne pas cliquer trop vite sur des liens. Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur.

Ne jamais utiliser un compte administrateur pour naviguer. L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci. Ces droits permettent ou non de conduire certaines actions et d'accéder à certains fichiers d'un ordinateur. On distingue généralement les droits dits d'administrateur et les droits dits de simple utilisateur. Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou surfer sur l'Internet. En limitant les droits d'un utilisateur, on limite aussi les risques d'infection ou de compromission de l'ordinateur.

Contrôler la diffusion d'informations personnelles. L'Internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse échappent instantanément ! Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles sur des sites qui n'offrent pas toutes les garanties requises. Dans le doute, mieux vaut s'abstenir…

Ne jamais relayer des canulars. Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc. Quel que soit l'expéditeur, rediffuser ces messages risque d'induire des confusions et de saturer les réseaux.

Soyez prudent : Si par exemple un correspondant bien connu et avec qui l'on échange régulièrement du courrier en français, fait parvenir un message avec un titre en anglais (ou toute autre langue) il convient de ne pas l'ouvrir. **En cas de doute, il est toujours possible de confirmer le message en téléphonant.**

Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants. Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .pif (comme une pièce jointe appelée photos.pif) ; .com ; .bat ; .exe ; .vbs ; .lnk. À l'inverse, quand vous envoyez des fichiers en pièces jointes à des courriels privilégiez l'envoi de pièces jointes au format le plus « inerte » possible, comme RTF ou PDF par exemple. Cela limite les risques de fuites d'informations.

Source https://www.ssi.gouv.fr/entreprise/precautions-elementaires/dix-regles-de-base/