Sécurité

Sommaire

Introduction

La sécurité informatique devient de plus en plus préoccupantes. Régulièrement, on entend parler de fuites de données, d'entreprises piratées. Et les conséquences peuvent être dévastatrices.

Il faut donc prendre conscience de cette menace et adopter les bons gestes pour se protéger et réduire les risques. Les pirates sont toujours à l'affût pour trouver des moyens d'accéder à nos données, et les sociétés de marketing ou les réseaux sociaux aussi.

Les menaces

Les menaces sont diverses. Fuites de données, perte d'accès à ses données, piratage, ransomware, phishing, espionnage. Tout système relié à internet est potentiellement vulnérable, et toute activité sur internet est potentiellement risquée si on ne se protège pas un minimum.

Dès que l'on utilise internet, on laisse des traces, des sites visités, de sa localisation, etc. Et cela donne des informations à d'éventuels pirates, ou à des sociétés de marketing (ou les réseaux sociaux comme Facebook, ou également Google) qui se servent de ses données pour nous pister.

Les bases pour se protéger

Pour se protéger, il existe quelques bonnes pratiques qui permettent de réduire les risques. Tout d'abord, toujours faire les mises à jour de son système et de ses logiciels, que se soit sur son ordinateur ou sur son smartphone. C'est la base.

Ensuite, avoir un antivirus à jour, sur son smartphone également.

Utiliser un firewall pour se protéger des intrusions sur votre système.

Utiliser un mot de passe fort (minuscule, majuscule, chiffre et ponctuation) et différent pour chaque site, c'est important.

Faire des sauvegardes de toutes ses données, régulièrement, sur plusieurs supports et si possible dans des lieux différents. En cas de ransomware, piratage ou simplement soucis matériel.

Voilà les principales techniques de sécurité à mettre en œuvre dès que l'on utilise un ordinateur, ou un smartphone.

Aller plus loin

Pour ce qui est des mots de passe, on peut utiliser un gestionnaire de mot de passe, comme KeepassX. Cela permet de créer des mots de passe fort mais aussi de les stocker de façon sécurisé.

Concernant les mails, il faut faire très attention au phishing. Pour chaque mail reçu, il faut bien vérifier l'adresse de l'expéditeur. Toujours être méfiant si on ne le connaît pas. Vérifier que les liens renvoient bien vers un domaine officiel, certains sont très proche et peuvent porter à confusion. Et bien sûr, ne jamais donner d'informations trop personnelles, et encore moins d'informations de paiement, par mail.

Afin de chiffrer vos mails, pour qu'ils ne soient lisible que par le destinataire, vous pouvez utiliser l'extension Enigmail avec le client Thunderbird, ou opter pour ProtonMail, un service de mail sécurisé.

On peut chiffrer ses données sur son disque dur afin de les protéger en cas de piratage ou d'intrusion. Il existe divers utilitaires pour cela. Le plus sécurisé est VeraCrypt.

Pour finir

La sécurité est l'affaire de tous. Chacun doit adopter ces bonnes pratiques pour se protéger et protéger les autres. Les GAFAM règnent en maître sur internet et utilise des techniques de plus en plus poussées pour pouvoir nous pister. Pour les pirates, c'est la même chose.

Prendre conscience de cela est déjà un pas en avant. Ensuite, il faut passer à la pratique en modifiant nos comportements, nos habitudes et outils afin de pouvoir se protéger des principales menaces.

Bibliographie

Cybersécurité : https://fr.wikipedia.org/wiki/Cybers%C3%A9curit%C3%A9
CNIL : https://www.cnil.fr/
ANSSI : https://www.ssi.gouv.fr/
MOOC cybersécurité de l'ANSSI : https://secnumacademie.gouv.fr/
Chiffrement des données : https://www.lebigdata.fr/chiffrement-des-donnees-tout-savoir
Firewall : https://www.commentcamarche.net/contents/992-firewall-pare-feu