Se protéger des malwares

Un malware (ou maliciel) est un logiciel malveillant qui infecte, à l'insu de l'utilisateur, les ordinateurs et objets connectés afin d'en perturber le fonctionnement.

Ce terme regroupe toute sorte de menaces informatiques qui ont des objectifs différents :

* Le virus : programme qui se copie à maintes reprises et infecte un ordinateur de manière à le rendre inutilisable
* Le cheval de Troie : application qui semble saine mais qui renferme un logiciel malveillant. Une fois l'application installée, le code malveillant fait son travail. La plupart du temps, l'utilisateur ne sait pas qu'il l'a installé
* Ver informatique : programme qui se propage sur un réseau pour créer des copies de lui-même sur d'autres PC
* Rançongiciel : logiciel qui bloque l'utilisation du PC. Il est alors demandé une rançon en échange du déblocage
* Spyware : logiciel d'espionnage qui récolte les informations personnelles de l'utilisateur et les renvoie à son auteur pour que celui-ci puisse les utiliser

Plusieurs indicateurs peuvent signaler une intrusion :

* L'appareil est subitement lent ou surcharge sans motif
* Des fenêtres publicitaires apparaissent continuellement
* Vous constatez du SPAM sur l'appareil
* L'appareil n'arrête pas de redémarrer
* Des messages d'erreur étranges se manifestent
* L'antivirus est désactivé sans raison

Se protéger efficacement des malwares :

1. Mettre à jour son système d'exploitation
La plupart des mises à jour servent à combler des failles de sécurité. Il est donc important de bien mettre à jour le système d'exploitation.

2. Faire preuve de vigilance
Évitez les liens douteux que vous recevez et les messages électroniques inconnus. Votre banque ne vous demandera jamais des données personnelles par mail, par exemple.

3. Éviter les sites à risques
Les sites à caractères pornographiques, les cracks, les P2P sont les plus souvent infectés par des Malwares.

4. Bloquer les publicités
Derrière des publicités peuvent se cacher des logiciels malveillants. Évitez de cliquer sur des bannières publicitaires.

5. Mettre à jour l'ensemble des logiciels de l'appareil
Comme le système d'exploitation, les logiciels présents sur l'ordinateur ont besoin d'être mis à jour afin de combler des failles de sécurité.

6. Utiliser des mots de passe différents et efficaces

Il sera plus difficile pour le pirate de récolter vos différentes données si vous utilisez de multiples mots de passe et si ceux-ci sont forts en sécurité. Cet article, sur le site "Les Numériques", vous informe des 100 mots de passe les plus piratés en 2017 (et donc, à éviter).

7. Utiliser les sources sûres
Téléchargez des programmes sur les sites de sources sûres et, de préférence, sur les sites officiels.

8. Créer un 2e profil sur son ordinateur
Ce 2e profil sera utilisé pour vos besoins quotidiens et aura des droits restreints. Ce qui limitera les dégâts en cas d'attaque d'un logiciel malveillant.

9. Nettoyer régulièrement son système
Il y a peut-être des fichiers à risque dans les fichiers inutilisés ou indésirables. Un nettoyage régulier du système permet de supprimer les fichiers inutiles.

10. Utiliser un antivirus qui protégera des malwares