

Malware

« Malware » est un terme générique qui renvoi au software malveillant qui infiltre et infecte l'ordinateur à l'insu du propriétaire.

Il existe différents types de malware :

- **Police ransomware** = faux message des forces de l'ordre qui apparait sur votre écran et qui vous accuse d'avoir visité des sites web illégaux. Ce malware peut bloquer votre appareil en chiffrant vos données, et demande alors que vous payez pour les débloquer. Les tablettes et smartphones peuvent également être soumis à ce genre de ransomware. Gardez à l'esprit que la police ne vous demanderait jamais une « rançon » de telle manière.
- **Adware** = ou publiciel, est un logiciel qui remporte de l'argent en affichant des publicités intempestives sur l'appareil de l'utilisateur. Une part du logiciel est utile et incite donc l'utilisateur à l'installer, l'autre part s'occupe d'afficher la publicité. Contrairement à d'autres logiciels malveillants, le publiciel ne permet pas de voler des données ou de contrôler l'appareil à distance.
- **Spyware** = logiciel espion qui rassemble des informations (sites web visités, adresse IP, etc.) pour les transmettre aux malfaiteurs intéressés.
- **Browser hijacking malware** = logiciel qui modifie les paramètres du navigateur et impose par exemple un nouveau moteur de recherche, qui va permettre à l'auteur de se faire du profit via des publicités. Le logiciel peut également changer la page d'accueil, installer des barres d'outils, des barres de recherches, etc.
- **Virus** = logiciel qui se reproduit et se propage (par des clés USB, téléchargements, mails, etc.) sur d'autres appareils en s'insérant dans un logiciel légitime (hôte). Le virus peut endommager l'ordinateur en infectant les fichiers sur la mémoire vive ainsi que sur le disque dur, en supprimant des données, en utilisant toute la mémoire, etc.

Présentation

Base légale

Art. 550*bis* et 550*ter* du Code pénal
Art. 2, 3, 4 de la Convention de Budapest (4)

Conseils

- Installez un anti-virus et un anti-malware, faites un scan régulièrement
- Installez les mises à jour de votre ordinateur et vos programmes
- Ne téléchargez que de sources fiables
- Faites régulièrement une copie de vos données sur un disque dur externe
- Ne cliquez pas sur des popups, bannières, des liens ou des annexes dans des mails si vous ne connaissez pas l'expéditeur ni ce que contient l'annexe
- Ne téléchargez pas d'applications de sources inconnues. Dans Android, gardez la fonction « unknown sources » désactivée et la fonction « verify apps » activée
- Faites un scan des clés USB ou autres appareils externes avant de les utiliser
- Si vous avez été victime de malware, signalez-le à la police locale

Liens utiles

<https://www.microsoft.com/fr-fr/security/pc-security/virus-what-is.aspx>
<http://windows.microsoft.com/fr-fr/windows/how-remove-computer-virus#how-remove-computer-virus=windows-7>