

Conseils sécurité

Vous trouverez ici des conseils pour améliorer la sécurité de votre ordinateur (*logiciels, comportements de l'utilisateur, ...*). Le but de ce document n'est pas de savoir supprimer les virus ou autres logiciels malveillants, mais d'éviter leur installation sur votre PC.

« *Il vaut mieux prévenir que guérir* ».

Sommaire :

[Qui sont-ils](#)

[Le comportement de l'utilisateur](#)

[Les logiciels](#)

I. [Qui sont-ils ?](#)

Avant de savoir comment, il est nécessaire de savoir qu'il existe différents type de logiciels malveillants.

A. Virus

Un **virus** informatique est un logiciel malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes. (Source : [Wikipédia](#))

B. Spyware

Les **logiciels espions** ou (*spyware*) est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. (Source : [Wikipédia](#))

C. Spam

Le **spam**, (*pourriel ou pollurriel*) est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. (Source : [Wikipédia](#))

D. Phishing

L'hameçonnage, (*ou phishing*) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. (Source : [Wikipédia](#))

E. Hoax

En informatique, les **canulars** (*appelés en anglais hoaxes, pluriel de hoax*) se trouvent souvent sous la forme de courriel ou de simple lettre-chaîne. (Source : [Wikipédia](#))



F. Ver

Un **ver informatique** est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. (Source : [Wikipédia](#))

G. Cheval de Troie

Un **cheval de Troie** (*Trojan Horse en anglais*) est un logiciel d'apparence légitime, conçu pour exécuter des actions à l'insu de l'utilisateur. Il est souvent utilisé pour prendre le contrôle de l'ordinateur infecté sans que l'utilisateur en ait connaissance. (Source : [Wikipédia](#))

H. Keylogger

Un **keylogger** (*littéralement enregistreur de touches*) est un dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage. (Source : [Comment ça marche](#))

I. Rogues

Un **rogue** est un faux logiciel de protection qui prétend que votre ordi est infecté, en général, un faux antivirus apparaît qui fait un scan (très rapide) et affiche des détections qui sont fausses. Le but est de vous faire acheter ce faux antivirus. (Source : [Comment ça marche](#))

Passons à la pratique.

II. Le comportement de l'utilisateur

L'utilisateur est le meilleur antivirus pour l'ordinateur. Suivez ces quelques préceptes et votre Pc vous remerciera.

A. Un bloqueur de pub vous installerez

Lorsque vous naviguez sur Internet, utilisez un bloqueur de pub. Je vous conseille fortement [uBlock Origin](#), qui est mieux qu'Adblock.

B. Avec méfiance vous téléchargerez

Ne pas télécharger n'importe où. Si vous téléchargez que cela soit, pour installer un nouveau logiciel ou télécharger un film, un jeu, (*n'oubliez pas que ces dernières pratiques sont interdites*), vérifiez où vous téléchargez. Utilisez des sites connus et reconnus, pour éviter d'installer autre chose que ce que vous vouliez installer.

C. A l'installation, d'intelligence vous ferez preuve

Lorsque vous installez un logiciel, vous ne cliquez pas sur **Suivant**, sans réfléchir. Lisez un minimum, en effet, des logiciels publicitaires, peuvent s'installer en même temps que votre logiciel.



D. Des mails vous vous méfiez

Lorsque vous recevez un mail, vérifiez bien qui est votre expéditeur. Il arrive que vous receviez des mails de votre banque, de votre site d'achat préféré, **ne jamais cliquer sur les liens présents sur les mails.**

En effet, bon nombre de mails sont des faux, ils imitent les mails de votre banque (*logo, mise en page, ...*) afin de vous envoyer sur un faux site, qui ressemble à s'y méprendre au site de votre banque. Si vous cliquez sur le lien, vous allez être redirigé avec un faux site, qui ressemble lui aussi au site en question, sauf que lorsque vous allez indiquer vos identifiants, vous ne pourrez pas vous connecter. Mais vos identifiants seront sauvegardés dans l'ordinateur des pirates. Une fois vos identifiants acquis, ils pourront aller sur votre compte, en se faisant passer pour vous. Cette technique s'appelle le [phishing](#).

Pour éviter cette mésaventure, ouvrez votre navigateur (*Firefox, Google Chrome*) et allez directement sur le site qui vous a envoyé le mail. Il y aura obligatoirement le bon de réduction, ou la promotion promis sur le mail. S'il n'y est pas, c'est que ce mail était un faux.

Autre astuce pour vérifier si le mail n'est une tentative d'escroquerie, regardez l'orthographe, car souvent les pirates ne sont pas français et il y a souvent des fautes d'orthographe.

E. À jour votre Pc restera

Maintenez votre système d'exploitation et vos logiciels à jour. Les mises à jour permettent de combler des failles de sécurité et résoudre des bugs.

Si votre système ou vos logiciels ne sont pas à jour, les pirates pourront utiliser cette faille de sécurité pour accéder à votre PC.

Tous les logiciels doivent être à jour et évidemment votre système d'exploitation (*Windows 7, 8.1 ou 10*).

Pour les mises à jour de votre système d'exploitation, c'est Windows Update, qui gère les mises à jour, sans problème normalement.

Pour les logiciels, je vous conseille d'utiliser un logiciel qui va vérifier la présence de mise à jour de vos logiciels. Il existe différents outils : [Update Checker](#) ou [Secunia](#).

Update Checker est simple, en français et rapide. Si vous utilisez **Glary Utilities**, il y a un outil qui vérifie la présence d'une nouvelle version de vos logiciels.

F. Avec précaution une clé USB vous brancherez

Attention aux clés USB ! Les clés USB peuvent aussi être infectées et contaminées tous les PC auxquelles elles seront connectées.

Veillez à désactiver l'exécution automatique (ici pour [Windows 7](#) et ici pour [Windows 10](#)).

Pensez également à activer l'analyse des supports USB (*disques et clés USB*) de votre antivirus.



G. Les extensions vous afficherez

Les fichiers ont tous une extension qui permet à votre ordinateur de savoir à quoi correspond ce fichier :

- .exe = Logiciel
- .doc = Fichier texte (*Word, OpenOffice, LibreOffice*)
- .pdf = Document
- .avi = Vidéo
- .mp3 = Musique

Voilà un exemple, des extensions utilisez le plus souvent.

Si vous téléchargez une chanson avec l'extension de fichier **.exe**, c'est un virus, car une chanson l'extension est **.mp3**.

Mais par défaut, Windows cache les extensions de fichier. Pour les [afficher regardez ici](#).

III. Les logiciels

A. Les antivirus

Tout le monde le connaît l'antivirus, permet d'éviter que votre PC ne soit infecté par des logiciels malveillants (*virus, spyware, trojan, ...*) C'est la protection obligatoire à avoir sur tous les PC.

Il existe de très nombreux antivirus, payants, gratuits, avec ou sans protection en temps réel, des efficaces et des moins bons. Lequel choisir ?

Ceci n'est que mon point de vue, je ne trouve pas nécessaire d'acheter un antivirus. Si vous avez un comportement responsable sur Internet, si vous appliquez les conseils que je vous ai donnés plus haut, vous n'avez pas besoin d'un antivirus, surpuissant, qui va ralentir votre PC.

Avec **Windows 10**, Microsoft a mis Windows Defender par défaut. Je trouve qu'il est largement suffisant, les mises à jour ce font directement via Windows Update, votre antivirus sera donc à jour.

Si vous n'avez pas Windows 10, vous pouvez utiliser soit **Microsoft Security Essential** ou **Panda Cloud**. Ces deux antivirus, surveillent votre PC en temps réel et ne ralentissent pas trop votre PC.

Un seul antivirus avec protection en temps réel est suffisant.

Il existe aussi des antivirus, qui n'ont pas de protection en temps réel. Ils permettent uniquement de faire des analyses à la demande afin de vérifier si le PC n'est pas infecté.

Si vous avez un doute concernant la santé de votre PC, vous pensez qu'il est peut-être infecté, n'hésitez pas à faire une analyse avec un autre antivirus. Attention, on n'installe qu'un antivirus par machine, sinon, ça va être la très grosse pagaille.



Je vous conseille d'utiliser les antivirus en ligne, si sont généralement gratuit et qui font partis des Géant des antivirus. Je vous donne trois antivirus en ligne, qui fonctionnent super bien :

- [Eset Online Scanner](#)
- [BitDefender](#)
- [Trend Micro](#)

Si vous avez un doute concernant un fichier que vous avez téléchargé, ou qu'on vous a donné sur une clé USB, vous pouvez analyser ce fichier via **VirusTotal**. Ce site, analyse votre fichier avec plusieurs antivirus, afin d'avoir le résultat le plus fiable possible. Cliquez ici pour visiter [VirusTotal](#).

B. Les autres logiciels de protection

Malheureusement, aucun logiciel n'est infaillible, je vous conseille donc d'installer un autre logiciel en plus de votre antivirus : [Malwarebyte Anti-Malware](#). Malwarebyte, est un logiciel qui analyse à la demande soit votre disque dur entier, soit un fichier en particulier.

Un **pare-feu** (*appelé aussi coupe-feu, garde-barrière ou firewall en anglais*), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). (*Source : [Comment ça marche](#)*)

Le pare-feu était plus qu'indispensable avec Windows XP, mais aujourd'hui, Windows 7, 8.1 et 10, dispose d'un pare-feu satisfaisant.

Pour autant, vous pouvez installer [Glasswire](#), qui est un pare-feu avec une jolie interface qui vous indique quels logiciels utilisent Internet. Il vous permet également de bloquer certains logiciels pour qu'ils n'accèdent pas à Internet.

Ce document est certes un peu long, mais je vous assure que si vous suivez ces quelques règles, naviguer sur Internet ne sera que bonheur.

En espérant vous avoir aidé. N'hésitez à me retrouver sur mon site [Logiciels Gratuits – Tutos.com](#)