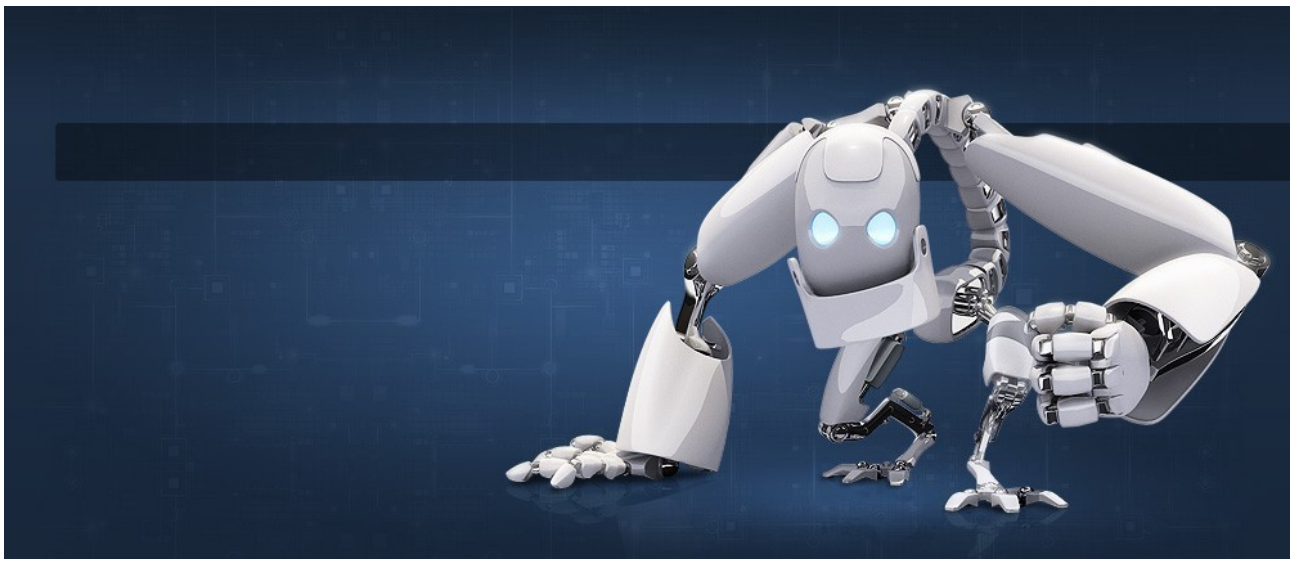


Comment donc ouvrir son ordinateur à Internet sans se laisser infecter immédiatement ? Quelques conseils de base...

Il existe toute une série d'indices qui peuvent indiquer l'infection de l'ordinateur par exemple:

- L'affichage à l'écran de messages ou de dessins inhabituels
- L'émission de sons étranges
- L'ouverture et la fermeture inattendue du lecteur de CD-ROM
- Le lancement aléatoire d'une application quelconque sans l'intervention de l'utilisateur
- L'affichage par le pare-feu de messages d'alerte annonçant qu'un logiciel installé sur l'ordinateur tente de se connecter à Internet sans que l'utilisateur soit à l'origine d'un tel comportement
- Vos amis ou vos connaissances parlent de vos messages alors que vous ne leur avez rien envoyé
- La boîte aux lettres contient énormément de messages sans objet et sans adresse d'expéditeur.
- Gel et échecs fréquents dans le fonctionnement de l'ordinateur
- Lenteur au moment du lancement des logiciels
- Impossibilité de charger le système d'exploitation
- Disparition de fichiers et de répertoires ou altération de leur contenu
- Requêtes fréquentes vers le disque dur (la petite lampe sur la tour clignote fréquemment)
- Microsoft Internet Explorer "gèle" ou se comporte bizarrement

Pourquoi ces infections/menaces ?

L'argent est le facteur principal de la motivation des créateurs de programmes malveillants.
Aujourd'hui, ces programmes sont source de revenus et les moyens sont divers

- Attaque en masse à partir d'ordinateurs détournés,
- Envois de publicités mails à partir d'ordinateurs détournés (spam),
- Affichage de publicités (adware),
- Arnaques avec de faux logiciels de sécurité (rogues),
- Vol de données, de mots de passe, de numéros de série de logiciels...
- Redirection vers des sites frauduleux (phishing),
- Chantage (ransomware),
- etc…

D'où proviennent-elles ?

- Les principaux vecteurs d'infections ou de menaces sont:
- Les cracks et les keygens
- Les faux codecs et ActiveX
- Les logiciels gratuits
- Les rogues, les faux logiciels de sécurité
- La navigation sur des sites à haut risque d'infections
- Les pièces jointes aux e-mails
- Les vers par les messageries instantanées
- Les hoax et le phishing

Comment les attrapons nous ?

Certains sites volontairement mal conçus permettent d'exploiter les failles, les vulnérabilités de votre ordinateur ou de vos logiciels.

Toutefois et dans la très grosse majorité des cas, c'est l'utilisateur lui-même qui invite sans le savoir des compagnons malveillants par un excès de confiance. Un seul clic suffit à votre malheur…

Le firewall / Pare feu

Qu'est-ce qu'un firewall ?

Un firewall ou pare-feu Internet est une solution matérielle ou logicielle qui bloque des attaques en provenance de pirates, de certains types de virus et de vers qui peuvent infecter votre ordinateur.

Si vous travaillez à domicile ou dans une petite entreprise, l'installation d'un pare-feu est la procédure la plus importante et la plus efficace pour protéger votre ordinateur.

Le pare-feu est le meilleur moyen de maitriser ce qui rentre et sort de votre ordinateur en évitant ainsi un certain nombre d'attaque et de génération de virus.

Son fonctionnement

La première fois que vous utilisez un produit se connectant à Internet (navigateur,client de messagerie, jeux en ligne, etc...), le pare-feu (logiciel) vous demande d'autoriser ou de refuser la connexion si celui-ci est en mode apprentissage.
Vous pouvez répondre ponctuellement Oui, ou demander que cette autorisation soit définitive. Les modalités peuvent être variables d'un pare-feu à l'autre suivant la configuration de ce dernier.

Il est important de lire les messages que vous indiquent votre pare-feu et ne pas répondre Oui si l'avertissement ne correspond pas à un programme que vous êtes en train d'utiliser.

De même, si le pare-feu vous avertit d'une tentative de connexion entrante, même sur un programme connu, en règle quasi générale vous devez répondre Non.
Ce type de message peut parfois apparaitre durant l'utilisation d'un logiciel de partage comme les logiciels d'échange de fichiers type P2P.

Le modem-routeur (box) de mon fournisseur possède déjà un Pare feu, dois-je en installer un sur mon ordinateur ?

La réponse est simple. Il faut également installer un pare-feu sur l'ordinateur.

En effet les pare-feux des routeurs ne bloquent que les intrusions.
Donc si vous avez un spyware sur votre ordinateur rien ne l'empêchera de communiquer des renseignements privés vers un site frauduleux.

Certes il y a moyen de filtrer les sorties avec un pare-feu de routeur (voir la notice de votre appareil pour les détails) mais cela pose des problèmes difficilement surmontables pour les protocoles qui assignent dynamiquement des ports variables, comme le FTP.
C'est donc à déconseiller, sauf pour un utilisateur très averti et expérimenté.
De plus, même avec un filtrage en sortie rien n'empêche un spyware de communiquer par un port autorisé.

Les pare-feux logiciels constituent donc un complément indispensable car ils filtrent les sorties en reconnaissant les programmes que vous avez autorisés à communiquer avec l'extérieur.
Toutefois certains malwares sont capables de désactiver certains pare-feu, ce qui leur est impossible de faire pour les pare-feux des routeurs.
Comme les deux types de pare-feux agissent à des niveaux très différents leur coopération constitue un rempart très efficace.

L’ anti-virus

Le logiciel anti-virus est un élément absolument nécessaire pour obtenir un niveau de sécurité maximal.
Il est le gardien de votre ordinateur et de son contenu (veille à sa santé, le protège des virus, répare les dégâts en cas d'infection en fonction de la nature du virus)
Un anti-virus performant utilisant plusieurs méthodes de détection est vivement conseillé. Celui-ci permettra de détecter les virus connus, mais aussi inconnus par une analyse comportementale.

Voici les méthodes d’analyse les plus efficaces et conseillées pour prévenir l’intrusion de programmes dangereux.

Analyse par signature

Les éditeurs antivirus ayant préalablement identifié et enregistré des informations sur le virus, comme le ferait un dictionnaire, le logiciel peut ainsi détecter et localiser la présence d’un virus.

Lorsque cela se produit, l'antivirus dispose de 2 options, il peut :

Tenter de réparer les fichiers endommagés en éliminant le virus ; Supprimer les fichiers contaminés.

Afin de maximiser le rendement de l'antivirus, il est essentiel d’effectuer de fréquentes mises à jour afin d’obtenir les dernières signatures de la part de l’éditeur.

Généralement, les antivirus examinent chaque fichier lorsqu'il est créé, ouvert, fermé ou lu (en fonction du paramétrage). De cette manière, les virus peuvent être identifiés immédiatement.

Même si les logiciels antivirus sont très performants et régulièrement mis à jour, les créateurs de virus font tout aussi souvent preuve d'inventivité. En particulier, les virus «oligomorphiques», «polymorphiques» et plus récemment, «métamorphiques», sont plus difficiles à détecter.

Analyse du comportement (Pro active)

Afin de détecter les nouvelles générations de virus, ce type d’analyse consiste à détecter les comportements suspects des programmes.
Par exemple, si un programme tente d’écrire des données sur un programme exécuté, l’antivirus détectera ce comportement suspect et en avisera l’usager qui lui indiquera les mesures à suivre.

Contrairement à l'approche précédente, la méthode du comportement suspect permet d'identifier des virus très récents qui ne seraient pas encore connus dans les signatures de l'antivirus.
Toutefois, le fait que les usagers soient constamment avertis, de fausses alertes peuvent les rendre insensibles aux véritables menaces. Si les usagers répondent « Accepter » à toutes ces alertes, l'antivirus ne leur procurera aucune protection supplémentaire.

Analyse heuristique

L'analyse heuristique est utilisée par la plupart des éditeurs à l'heure actuelle.

Par exemple, l'antivirus peut analyser le début de chaque code de toutes les nouvelles applications avant de transférer le contrôle à l'usager.
Si le programme semble être un virus, alors l'usager en sera averti.

Toutefois, cette méthode peut également mener à de fausses alertes. La méthode heuristique permet de détecter des variantes de virus et, en communiquant automatiquement les résultats de l'analyse à l'éditeur, celui-ci peut en vérifier la justesse et mettre à jour sa base de définitions virales.

La méthode heuristique consiste à émuler le système d'exploitation et à exécuter le fichier lors de cette simulation. Une fois que le programme prend fin, les logiciels analysent le résultat afin de détecter les changements qui pourraient contenir des virus.

En raison des problèmes de performance, ce type de détection a lieu habituellement pendant l'analyse à la demande.
Les principaux antivirus du marché se concentrent sur des fichiers de signatures et comparent alors la signature virale du virus aux codes à vérifier.

Analyse par Cloud Computing

Le cloud computing, informatique en nuage ou infonuagique est un concept qui consiste à déporter sur des serveurs distants des traitements informatiques traditionnellement localisés sur des serveurs locaux ou sur le poste client de l'utilisateur.

Certains antivirus ne fonctionnent qu'avec cette méthode, ce qui implique d'avoir l'accès continu à internet. Le moteur d'analyse ne se trouvent plus sur le PC mais décentralisés, sur les serveurs de la société éditrice.
Ainsi, l'antivirus ne consomme que très peu de ressources système, et aucune mise à jour n'est nécessaire, contrairement aux antivirus classiques.

Votre système d’exploitation

Pour infecter votre ordinateur, les auteurs des menaces peuvent s'appuyer sur des failles de sécurité de votre système d’exploitation. Une faille de sécurité est un comportement non prévu par une application qui peut permettre de compromettre le système.

Il existe deux types de failles :

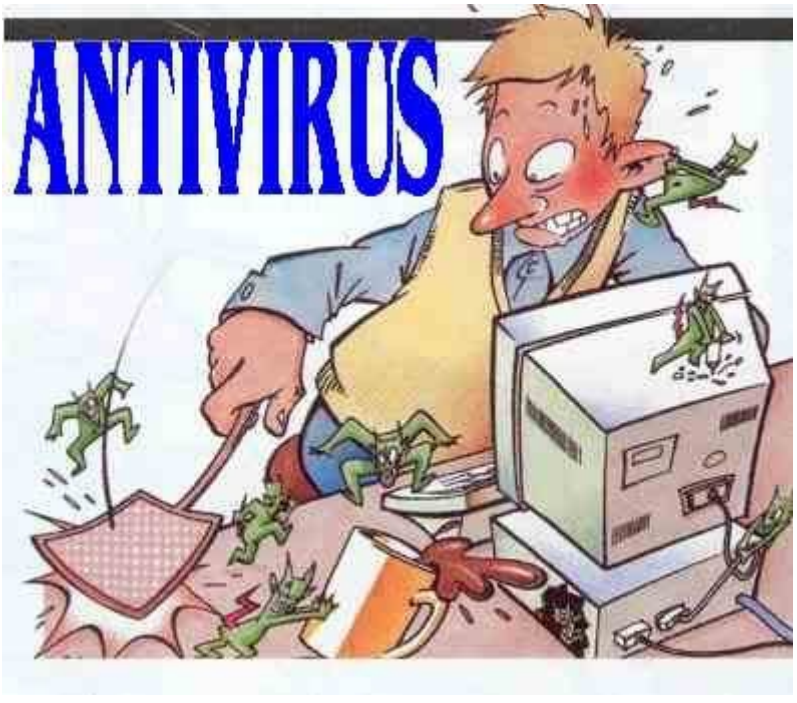
Les failles distantes :

celles-ci sont exploitables à distance, c'est à dire via un accès distant de l'ordinateur et sans interaction de l'utilisateur. Ce sont bien entendu, les plus dangereuses puisqu'elles peuvent permettre la compromission du système à tout instant.

Les failles locales :

celles-ci sont exploitables seulement par l'interaction de l'utilisateur, par exemple lors de la consultation d'un site WEB qui exploite une faille sur le navigateur ou lors de l'ouverture d'un fichier vidéo ou audio prévu pour exploiter une faille sur le lecteur audio/vidéo.

A l'heure actuelle, les failles de sécurité les plus exploitées sont celles contenues sur les navigateurs WEB (surtout Internet Explorer 6), des milliers de sites WEB sont piratés (phishing ou defacing) en permanence.
L'internaute qui tombe dessus et dont le navigateur WEB est vulnérable exécute alors automatiquement et à son insu le code malicieux, l'infection s'installe alors.



Je vous invite à appliquer les recommandations suivantes

Maintenir son système à jour

Les mises à jour régulières de votre système d'exploitation permettent de combler et corriger les failles de sécurité ainsi que les bugs pouvant être utilisés par des personnes malveillantes afin de compromettre l'intégrité et la sécurité de votre système d'exploitation. Ces mises à jour sont primordiales !

- **Comment savoir si mon ordinateur est à jour ?**
- **Activer les mises à jour automatiques**

Maintenir ses logiciels à jour

Il est important de maintenir à jour tous vos logiciels en particulier les composants de vos navigateurs, ainsi que vos lecteurs vidéos/audio : Java, Flash, QuickTime, etc...

Favoriser l'accès à Internet avec des droits limités

Dans les dernières versions de Windows il est possible de limiter les droits octroyés aux différents utilisateurs (installation d'un programme par exemple).

Le problème est que par défaut la session est habituellement ouverte en mode administrateur (mode ou tout est possible) ce qui fait qu'un malware s'introduisant dans l'ordinateur héritera lui aussi des droits de l'administrateur.

- **Créer un utilisateur standard avec Windows XP**
- **Créer un utilisateur standard avec Windows Vista**
- **Configuration de Windows 7 pour un compte d'utilisateur limité**

Utiliser Internet avec des programmes plus sûrs

Internet Explorer et Outlook Express (Windows Mail) sont les programmes les plus visés par les pirates. En outre ils incorporent la technologie ActiveX ce qui les rend potentiellement vulnérables.
Vous améliorerez grandement votre sécurité en utilisant comme navigateur Firefox, et Thunderbird comme programme de courrier.

- **Firefox**
- **Thunderbird**

Protégez vous des infections par supports externes.

USB-set est un logiciel destiné à vous aider à configurer votre PC pour limiter les risques de propagation des infections par supports amovibles entre votre PC et ces supports. Attention, ce logiciel ne permet en aucun cas de supprimer une infection de ce type si elle est déjà active, il s'agit avant tout d'un outil de prévention.

- **USB-set**

Faites très attention aux téléchargements d'Internet.

Si jamais vous découvrez un fichier suspect sur votre ordinateur ou pensez qu'un programme téléchargé depuis Internet est malicieux, vous pouvez vérifier ces fichiers à partir du site VirusTotal, de même que vous pouvez soumettre l'adresse url d'un site suspect.

- **Analyse de fichiers suspects**

Ne pas croire aux optimiseurs miracles et nettoyeurs en tout genres.

Beaucoup de ces programmes miracles, parfois "Partenaire de microsoft" font plus de mal que de bien....

- **Les nettoyages du registre sont-ils nécessaires ?**

Conclusion

- N'ouvrez aucune pièce jointe dans un e-mail venant d'un expéditeur inconnu ou incertain.

- N'ouvrez aucun message e-mail si vous ne savez pas de quoi il s'agit, même s'il est envoyé par un ami ou un partenaire. 80% des virus se répandent par courrier électronique. Il est plus facile de prévenir que de réparer, c'est pourquoi il est conseillé de demander une confirmation de l'envoyeur.

- N'ouvrez pas les fichiers ou messages attachés ayant un objet suspect ou inattendu. Si vous voulez les ouvrir, sauvegardez-les sur votre disque dur et analysez-les avec un antivirus mis à jour.

- Effacez tout mail en chaîne ou message non désiré. Ne les transmettez pas et ne répondez pas aux envoyeurs. Ce type de message est considéré comme un spam, parce qu'il s'agit d'informations non désirées et non sollicitées, affectant le trafic Internet.

- Ne copiez aucun fichier si vous ne connaissez ou ne faites pas confiance à sa source.

- Faites très attention aux téléchargements d'Internet. Vérifiez à chaque fois les sources et veillez à ce qu'un antivirus ait déjà vérifié les fichiers sur le site. Si vous n'en êtes pas certain, copiez le fichier sur votre disque dur et analysez-le avec votre antivirus.

- Utilisez un programme antivirus performant et mettez-le à jour le plus souvent possible. Choisissez un antivirus comportant un module résident, pour pouvoir surveiller l'activité de l'ordinateur pendant que vous travaillez.

- Évitez le phishing. Votre banque, compagnie d'assurance, service de paiement en ligne,ne vous contacteront jamais par mail pour vous demander vos mots de passe, vos coordonnées de carte bancaires, même si ces messages vous paraissent bien imités et vous offrent de cliquer sur un lien qui semble être de celui de la banque.

Australien de Nîmes.