

Les Anti-virus

Qu'est qu'un Virus ?

Un virus informatique est un logiciel malveillant **conçu** pour se propager à d'autres ordinateurs en s'insérant dans des programmes et dans le système.

Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques (internet, intranet), les clefs USB, etc.

Comment les éviter et les combattre ?

Le meilleur moyen de ne pas être infecté par des virus est avant tout de savoir où l'on va sur internet et faire attention aux courriers reçus dans sa boîte e-mail (même provenant de personnes qu'on connaît bien !).

Il faut donc être attentif au contenu des e-mails : vous ne serez jamais infecté si vous ne cliquez pas sur les **liens internet** contenus dans l'e-mail. Ces liens vous invitent souvent à gagner des sommes folles, des voyages fabuleux, d'obtenir du viagra ou d'autres médicaments/drogues à prix ridicules... etc. Comme dans la vie réelle, prenez vos précautions face aux arnaqueurs, leurs techniques sont différentes mais leur objectif reste le même.

Pour vous protéger des virus et les combattre, il faut installer un logiciel antivirus sur votre ordinateur. Il faut savoir que les vendeurs au moment de l'achat de votre ordinateur essaient de vous vendre un programme anti-virus lorsque des solutions gratuites existent et sont très efficaces. Une autre technique commerciale consiste à installer un antivirus payant mais valide que pour une courte période qui nécessite par la suite un paiement pour continuer à être utilisé. Une **solution anti-virus gratuite** est ce qu'il reste de mieux à faire pour ne pas se ruiner, tout en restant hautement protégé. Les programmes payants ne sont pas spécialement plus performants, et ils nécessitent de repayer une licence annuelle pour être protégés.

Les logiciels anti-virus gratuits les plus performants sont:

- 1) Avira Antivir
- 2) AVG
- 3) Avast



Le Spam

Le « spam » ou en français « pourriel » désigne l'envoi massif de messages non sollicités à de multiples destinataires. Il est le plus couramment associé au courrier électronique non-désirable, mais il s'applique aussi aux forums de discussion, à la messagerie instantanée, aux réseaux sociaux. Il existe des définitions juridiques différentes du spam selon les pays, et des approches diverses pour lutter contre ce fléau.

L'hameçonnage (ou obtention illicite d'informations), suscite de graves inquiétudes pour la sécurité des consommateurs. Cette technique consiste à envoyer à plusieurs destinataires des **messages** qui paraissent provenir d'une institution reconnue, telle une banque, le gouvernement, une grande entreprise. Ces messages contiennent souvent des liens vers de **faux sites web** qui vous invitent à donner des informations confidentielles et ainsi les collecter à des fins commerciales (vente de vos informations à des entreprises), ou parfois même frauduleuses (utilisation de votre carte de crédit). Le spam commercial est très répandu, car c'est un moyen efficace et bon marché d'atteindre un large public. Les adresses électroniques utilisées pour les envois en masse sont généralement collectées par des **robots** qui scrutent Internet et récupèrent les adresses qu'ils ont interceptées sur différents sites web.

Les «spammeurs» **profitent souvent de la bonne volonté et la crédulité des gens** pour récupérer les adresses de messagerie qui alimentent leurs bases de données.

Par exemple:

- Le texte du message annonce qu'une société ou une organisation promet qu'une certaine somme sera versée à chaque transfert du message.
- Le spam peut contenir des logiciels malveillants, toutefois **il n'a pas de chance d'infecter votre ordinateur si vous ne cliquez pas sur les liens vous y invitant dans le message.**
- Un autre type de fraude est baptisé "419" du nom de la loi nigériane qui punit ce type d'escroquerie. Le message promet en général le partage d'une somme d'argent importante à ceux qui aideraient à réaliser des transferts bancaires.
- Le spam peut également être utilisé pour des actes de sabotage en bombardement intempestivement des forums de discussion par des messages factices afin de provoquer leur engorgement, voir même de boîte email ciblée. (Imaginez-vous votre boîte aux lettres recevant 2 tonnes de courriers)

Le Spam

Comment éviter (un maximum) de recevoir des spams dans sa boîte ?

- **Utilisez différents comptes de courrier e-mail** pour vos différentes utilisations, afin d'éviter de donner votre adresse "personnelle" (pour s'inscrire sur un forum, remplir des formulaires, etc).
- Soyez vigilants quand vous recevez du courrier électronique. N'ouvrez pas les messages dont la source vous semble douteuse.
- Méfiez-vous particulièrement des **pièces jointes** et des **liens internet** dans les messages. Si vous n'attendez pas de pièce jointe d'un expéditeur, ou si vous avez un doute, ouvrez l'e-mail sans télécharger la pièce jointe, ni cliquer sur les liens. **Si vous connaissez** l'expéditeur, demandez lui si cet email était intentionnel et dans le cas contraire, le prévenir que sa boîte e-mail est infectée.
- **Vérifiez tous les liens présents dans les courriers électroniques avant de les ouvrir.** Il suffit de laisser votre curseur sur le lien (sans cliquer), et l'adresse internet doit apparaître dans le coin gauche en bas de votre écran. Si vous estimez que la destination d'un lien n'est pas celle qui est prétendue, saisissez ce lien dans votre navigateur au lieu de cliquer dessus pour l'ouvrir.
- **Utilisez des filtres antispam** pour ne pas consacrer trop de temps à la suppression des messages non sollicités. (Ils s'activent automatiquement dans les options de votre boîte email gmail, hotmail, yahoo...)
- **Évitez de diffuser** trop largement votre adresse de messagerie électronique. N'oubliez pas que, si vous entrez votre adresse de messagerie dans un site web, les robots peuvent l'intercepter et l'ajouter à des listes de distribution utilisées pour le spam.
- **Ne répondez pas aux spams.** Si vous le faites, vous confirmerez votre adresse de messagerie au spammeur. Les réponses automatiques du type «absent du bureau» posent un problème parce que ces messages répondent aussi bien aux spammeurs qu'aux destinataires autorisés.

Derniers conseils, derniers outils

Le plus important pour ne pas endommager votre système, **est d'empêcher tout fichier, dont vous ne connaissez pas la source, de rentrer sur votre disque dur.** Vous ne risquez pas que des fichiers rentrent dans votre ordinateur lorsque vous êtes en train de surfer si vous n'acceptez pas les téléchargements qu'ils proposent.

Si votre ordinateur a été infecté par un programme «indésirable», il existe des solutions pour le retirer proprement, et/ou l'empêcher d'infecter chaque partie de votre ordinateur. Les anti-virus ne peuvent malheureusement pas faire grand chose contre ce genre de petits programmes malveillants puisqu'ils arrivent sur votre ordinateur avec votre consentement, et qu'ils ne sont pas considérés comme étant un dangereux virus.

Pour protéger votre ordinateur de manière complémentaire, **vous pouvez installer un pare-feu.** Un pare-feu, aussi appelé **firewall** est un logiciel qui sert à gérer le trafic de votre connexion internet entrante et sortante. Il vous **permet de contrôler/filtrer** tout ce qui passe, mais ce type de programme nécessite une plus grande connaissance de l'informatique et ils sont plutôt réservés aux entreprises. **Aujourd'hui, les firewall sont de moins en moins nécessaires** puisqu'un contrôle du trafic est déjà actif sur votre modem/routeur qui bloque toutes intrusions extérieures dans votre ordinateur. (Attention ceci ne vaut pas pour les trojans et autres virus qui rentrent dans votre machines grâce à vous, même si vous avez l'impression que c'est à votre insu !)

Vous pouvez vous procurer gratuitement ces programmes:

CCleaner: Permet, grâce à une interface simplifiée, de gérer les programmes installés de nettoyer la mémoire temporaire de l'ordinateur (qui se surcharge au fil des mois), de protéger votre vie privée en vidant l'historique des navigations sur internet... et bien d'autres petits outils utiles.

Spybot: Logiciel qui vous permet de vous débarrasser des logiciels espions qui tentent de modifier la «base de registre» de votre ordinateur.

Malwarebytes: Ce logiciel de référence permet d'analyser votre système et d'effacer les logiciels malveillants (certains virus, «cheval de troie» et «vers»)

