

PC & INTERNET SECURITY



[Home](#)

[Sécurité PC & INTERNET](#)

[Search Engines](#)

[Webmaster](#)

[INTERNETSTUFF](#)

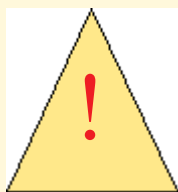
Anti-Virus:

[SYMANTEC](#)

[MCAFFEE](#)

[TREND MICRO](#)

[GATELOCK](#)



HOAX = FAUSSE ALERTE!

FAUSSE ALERTE = JETER à la POUBELLE!

L'OUVREZ JAMAIS DU COURRIER DE PERSONNES QUE VOUS NE CONNAISSEZ PAS!

TOOLS:

[IP TRACKING](#)

[Votre PC sur INTERNET](#)

[Glossaire Sécurité](#)

[Téléchargements](#)

[Contenu disque dur](#)



Good Links:

[SECUSER \(F\)](#)

[TOTAL PC1\(F\)](#)

[SCAREWARE\(D\)](#)

[ZONEALARM](#)

[ANTI-DIALER\(D\)](#)



Le mot < **HOAX** > vient de l'Anglais et veut dire < **FAUSSE ALERTE** >, < **CANULAR** > en français.

Probablement la plus part de vous ont déjà reçus un courrier électronique (**E-Mail**) envoyé par des amis ou des connaissances, vous alertant d'un nouveau **VIRUS!**

Vu l'importance de cette nouvelle et la confiance que vous apportez à vos amis, vous vous êtes lancés directement dedans pour relancer ce message à toutes vos connaissances; c.à.d.: Vous l'aviez envoyé à toutes les adresses marquées dans votre carnet d'adresses.

Eh bien, vos connaissances ont probablement eu le même réflexe que vous et ont envoyées ce message de la même manière, jusqu'à ce que le message de départ fasse plusieurs fois le tour du monde!

Au delà du fait que vous vous êtes fait piéger, sachez quand même que les < **HOAX** > contiennent des dangers!

!! LES FABRICANTS D'ANTI-VIRUS N'ENVOIENT JAMAIS DES E-MAILS NON SOLLICITÉS!!

Comme déjà défini ci-dessus les < **HOAX** > sont des messages contenant des < **FAUSSES ALERTES** >. Néanmoins quand ils sont envoyés il y a un effet **amplificateur**. (**EFFET DE BOULE DE NEIGE**).

Imaginez que le message reçu a une taille de 1kB (**Kilo Byte**) et que vous l'envoyez aux destinataires de votre carnet d'adresses (p.ex.: 30 personnes); il faut compter 30 x 1kB=30kB dans un paquet d'informations envoyés.

Imaginez maintenant que tout le monde qui a reçu le même message envoie ce message à autant ou plus de destinataires, le paquet d'informations augmentera tellement vite que les réseaux Internet seront encombrés.

Ceci peut même prendre l'envergure de bloquer totalement un réseau; car celui ci a aussi seulement une certaine capacité acceptable. (**largeur de bande**)!

Visualisez vous tout ceci comme une bouteille ou un récipient ou on essaye de verser un liquide à travers un entonnoir sans faire attention de la capacité de ce récipient.

Le récipient débordera.

Autre exemple: Imaginez vous que dans votre pays chaque citoyen envoie entre 30 et 50 cartes postales: Les services P&T seraient surchargés et plus rien ne fonctionnerait. C'est ce qui se passe quand tout le monde qui reçoit un courrier **HOAX** y répond en l'envoyant à d'autres personnes.

Autres < **HOAX** > bien connus:

Les **E-Mail** vous demandant d'envoyer ce mail à toutes vos connaissances contenant les textes suivants:

Un enfant est malade et nécessite le don d'un organe!

Les campagnes anti-guerre!

Et bien d'autres encore....

Quel effet cela a t'il concrètement?

Eh bien, tout simplement; plus qu'un réseau informatique est surchargé par trop de données y circulant, plus lentes deviendront les connexions!



*Des connexions plus lentes veulent dire que nous avons besoin de plus de temps pour visualiser un site Internet ou de faire un **téléchargement!** (DOWNLOAD).*

Plus de temps passé sur l'Internet veut dire aussi que nos connexions Internet vont devenir plus cher!

*C'est nous les **Internautes** qui payeront l'addition!*

*Les effets des **FAUSSES ALERTES:***

*Comme nous savons maintenant qu'il s'agit de **fausses alertes** nous ne faisons plus attention et le jour ou il y aura une vraie alerte virus, nous la manquerons du fait de **non-attention** au message!*

Mais soyez sans crainte. Si vraiment vous êtes intéressés pour être informés d'une apparition de nouvelles annonces de virus, vous pouvez vous abonner aux services Internet gratuits dont voici quelques liens intéressants:

[SECURITYMETRICS](#)

[SECUSER](#)

[TRENDMICRO](#)

*Les risques des **VIRUS CACHÉS:***

*Entre temps certains < **HOAX** > sont devenus tellement populaires et célèbres que des programmeurs malfaiteurs se sont appropriés ces messages en y adjoignant un **VIRUS!** La suite vous pouvez vous l'imaginer. Tous les messages envoyés contiennent le **VIRUS** et une vraie **épidémie informatique** se déclenche!*

CONCLUSION:

- 1. **Soyez toujours informés des nouvelles apparitions de VIRUS** en vous abonnant à un service gratuit comme mentionné ci-dessus. Vous recevez seulement un courrier électronique (**E-Mail**) dès qu'il y a un nouveau **VIRUS!***
- 2. **Soyez sûr** que vous avez installé un programme Anti-Virus récent et actualisé sur votre PC..*
- 3. **IGNOREZ** des courriers électroniques (**E-Mail**) de personnes que vous ne connaissez pas!*
- 4. **Si vous voulez vous rassurer** que le courrier reçu est un **HOAX** ou pas, utilisez les liens ci-dessous pour vous enseigner des dernières **rumeurs**.*

[HOAXBUSTERS](#)

[TOUS les HOAX en Français](#)

[TOUS les HOAX en Anglais](#)

Counter code has
changed. Please
update your code.

