Quelques conseils de base pour éviter la propagation des Virus

Comment *nettoyer* un courriel avant d'y répondre ou de le retransmettre

Vous êtes persuadés de pratiquer la bonne méthode pour envoyer des messages par Internet …
Mais vous vous demandez pourquoi vous avez des *VIRUS* ou des *SPAMS* !

Chaque fois que vous retransmettez un message, vous véhiculez des informations sur les personnes qui ont eu le message avant vous : leur nom ou surnom, mais surtout leur adresse de messagerie. Comme bien souvent le message est retransmis à d'autres, la liste des noms et adresses grossit, grossit, et fait boule de neige. Lorsqu'un virus pénètre dans cette liste, il atteindra tous ceux qui la composent, y compris vous-même. Il faut savoir que les virus peuvent s'incruster dans nos messages entre leur départ et leur arrivée.

Certains *récupèrent* ces adresses pour les revendre, ou ils vous envoient un courriel pour vous faire visiter leur site, gagnent 5 cent d'Euro par visite, mais vous, vous êtes piégés !

COMMENT POUVEZ-VOUS ARRETER CELA ?
Tout simplement par quelques précautions élémentaires :

1°) Lorsque vous faites suivre un message, après avoir cliqué sur " *Transférer* ", faites disparaître tous les **noms et adresses** des personnes qui ont déjà reçu le message. Vous les *noircissez* et les supprimez avec la touche *Suppr* : il est **IMPERATIF** de faire disparaître les noms et adresses de toute autre personne que vous, et celui à qui vous envoyez le message.

Seul le texte, ou le lien à retransmettre, doit figurer sur la page

Vous pouvez y ajouter votre propre texte ou votre signature, mais encore une fois il est essentiel de faire disparaître tous les noms et adresses de messagerie des personnes qui apparaissaient précédemment sur cette page.

2°) Lorsque vous faites un envoi groupé à plusieurs personnes, d'abord, vous avez intérêt à constituer un *groupe* dans votre carnet d'adresses, mais surtout, ne positionnez pas vos adresses dans la case " **A** " ou " **Cc** ", mais prenez l'habitude d'employer la case " **Cci** " (**Copie Cachée Invisible**).

De cette manière, seule la personne à qui vous écrivez verra ses coordonnées, mais pas celles des autres. Personne ne pourra relever ces adresses.

3°) Dans la ligne *Sujet*, enlevez toutes abréviations telles que *Fw* ou *Fwd* ou *Réf* ou autres, mais par contre, vous pouvez renommer le sujet si vous le désirez.

4°) Attention aux pièces jointes que vous envoyez, celles dont la référence de fichier se terminent par ".*exe*" sont les plus vulnérables et souvent détruites d'office par bon nombre d'antivirus.

Si vous êtes certains de leur *bonne santé* et que vous voulez impérativement les faire parvenir à quelqu'un, prenez la précaution de *zipper* votre dossier, qui voyagera ainsi en toute sécurité…

5°) Vous connaissez les *gifs*, qui accompagnent souvent nos courriels : il s'agit de petites bandes animées ou non, représentant toutes sortes d'animaux, de personnes ou d'objets, les plus connus étant le singe pendu par un bras (*monkey*), les papillons (*butterflies*) et le fameux Père Noël.

Il s'avère que le *gif* peut renfermer un ou des micro-fichiers servant à analyser votre utilisation d'internet et ainsi faire un ciblage fort intéressant pour le e-commerce. D'ailleurs, les sites offrant ces *gifs* fonctionnent grâce aux subsides de la publicité !

Si cela ne semble pas très inquiétant, il y a beaucoup plus grave : un *gif* peut contenir un virus genre trojan. En lisant un mail on ouvre, *par curiosité*, un *gif* mis en pièce jointe, et ***ALERTE : VIRUS*** **!** Ordinateur ralenti, connexions difficiles ou impossibles, etc… Les intrusions virales via le *gif* sont une menace sérieuse.

Pour ma part, je supprime toujours le *gif* quand je transfère un courriel ! C'est très simple : après avoir cliqué sur *transférer*, je *supprime* le *gif* dans la rubrique "*pièces jointes*". De même, je supprime au maximum les *gifs* qui se trouvent en bas des courriels avant de les transférer.