

Quelques règles de base pour protéger sa messagerie

0/ **Méfiez-vous de TOUS les messages que vous recevez.** Sans tomber dans la parano, il se peut que vous receviez un message d'une de vos **connaissances, dont la machine est infectée.** Soyez sur vos gardes, particulièrement lorsqu'il y a une **Pièce Jointe, s'il s'agit d'un message "Transmis" (Tr:) ou en "Réponse" (Re:)** à un de vos précédents messages, **que vous n'avez jamais envoyé !...** (voir **point 4** pour détail).

Essayez de voir dans la "**Source**" du message si votre correspondant vous invite formellement à voir la pièce jointe (voir **point 7** ci-dessous pour la manipulation)

Faites aussi attention à la **langue employée** par votre connaissance ou à tout autre "**détail inhabituel**"... (par exemple, un ami français vous écrit en anglais...)

1/ Pour éviter l'ouverture malencontreuse de messages non-désirés :

Désactivez les volets de visualisation. Vous savez ? Quand vous avez votre page de messagerie qui est en 2 parties : au-dessus, les messages reçus et dessous, la fenêtre qui vous permet de pré-visualiser vos messages = en fait vos messages sont Ouverts, donc **Activation (partielle ou totale) du virus ou du vers !!!**

Mode d'emploi pour désactiver les volets : Dans la fenêtre principale de votre messagerie (lorsque vous venez d'ouvrir votre messagerie pour la première fois), en haut à gauche, à côté de Fichier et Edition, sélectionnez **Affichage**, puis **Disposition**, puis **désactivez** la coche "**Afficher le volet de visualisation**".

2/ **Ne répondez JAMAIS à un message infecté ou à du Spam.** Sinon, cela prouve que votre adresse est active... (voir point 7). Contentez-vous de **supprimer le message.**

3/ Sous Windows :

a) **Mettez régulièrement à jour (~1x/s) votre Firewall (pare-feu) et Anti-virus,** sachant que certains virus désactivent les anti-virus...

b) **Mettez à jour votre PC et Téléchargez les patchs de Sécurité avec Windows Update.**

c) Si vous disposez de XP, **activez le Firewall (Démarrer, Connexions, Afficher toutes les connexions, clic droit sur l'icône Connexion, Propriétés, Paramètres avancés, Protéger mon ordinateur).**

d) **Faites fréquemment des Sauvegardes de vos dossiers sur disque ou disquette.**

e) **Créez des points de Restauration (Win 98/XP).** Cela vous permettra de récupérer vos données dans l'état qu'elles étaient Avant l'éventuel plantage. (Démarrer, Tous les programmes, Outils système, Restauration du système). **Attention ! Avant de créer ou de revenir à un point de restauration antérieur, Désactiver et Fermez les programmes en cours, y compris vos antivirus, firewall ou anti-espions !**

4/ **Bannissez les messages en Retour** (dans objet ou subject). La plupart des messages contenant des "Cochonneries" ont le **Re, Fw, Tr** faisant croire ainsi qu'il s'agit d'une "réponse" ou un "transfert" de message de la part de quelqu'un que l'on connaît ou pas...

Pour être précis, on peut effectivement faire des messages en retour, en cliquant sur "Répondre à" ou "Répondre à tous", mais il est préférable d'**enlever le "Re"** dans objet ou **mettre n'importe quel titre à la place** (Reprise, Retard, etc). Même si, actuellement, on ne peut plus vraiment se fier à ce genre d'indice.

5/ **Avant de surfer sur Internet**, créez dans votre messagerie un "Compte bidon", puis sélectionnez-le en tant que **Compte par défaut**. Ainsi, lorsque vous devez donner votre adresse sur des sites commerciaux, ils auront votre compte bidon et vous éviterez d'être victime de Spam.

N'oubliez pas de réactiver votre **Véritable compte par défaut** lorsque vous avez une **correspondance sérieuse** (ou lors de l'envoi de votre message, sélectionnez dans l'onglet "De", votre réel compte).

6/ **Pour éviter une propagation** au cas où votre PC serait infecté : dans votre Carnet d'Adresses, créez une ou plusieurs "Adresses Bidon" (par exemple : ac@abc.zz et 0123@123.yz). Ainsi, le virus ou ver qui voudra se propager, se stoppera à ces adresses sans-issues et évitera de s'envoyer avec tout votre carnet d'adresses.

7/ **Exemple de code dans un message infecté**

Ci-dessous, vous trouverez un exemple de code source avec lequel on peut détecter les messages dangereux. La plupart du temps, ils sont accompagnés d'une pièce jointe...

On peut lire dans Objet : "Test" ou "Hi" ou "Hello" ou "Undelivery message" ou "kfjdghgjhg" ou toute sorte de nom qui n'attire pas forcément l'attention...

En cas de suspicion, vous pouvez : cliquer (1x) avec le bouton droit de la souris sur le message qui n'a pas encore été ouvert, puis sur Propriétés, puis sur Détails.

Là, j'espère que vous ne verrez pas un code similaire à celui ci-dessous.

Entraînez-vous peut-être avec des messages Sûrs, au début... ;-)

ANALYSE

Dans "Return-Path", on constate que le message vient de Russie...

Dans "message Id" = nombre aléatoire d'envoi de messages...

En rouge : Auteur du virus (qui utilise des adresses multiples et cachées)

En rose : PC infecté (victime) qui a servi de "transfert" pour transmettre le (les) messages infectés

En vert : votre adresse

(code légèrement modifié)

```
Return-Path: <adress@ranflex.ru>
Received: from rue.mydnsboc2.bet (root@localhoste)
by votreserveur.com (8.11.6/2.101.6) with ESMTP id i13LaQb16572
for <vous@votreadresse>; Tue, 30 Feb 2004 12:30:16 -0300
X-ClientAddr: 70.122.235.42
Received: from localhost (APoatiers-105-1-4-16.w80-33.abo.wanadaa.com [70.14.250.46]) = PC
infecté !
by rue.mydnsboc2.bet (8.11.6/2.101.6) with ESMTP id i13LWNa16568
for vous@votreadresse; Tue, x Feb 2004 12:38:21 -0300
Date: Tue, 30 Feb 2004 12:38:21 -0300
Message-Id: <2003302032132.i13LWN16562@rue.mydnsbo2.bet>
From: "Elene" <Fu**enSu**id@IceMail.Com>
To: vous@votreadresse
```

Subject: *Important information for you. Read it immediately !*
MIME-Version: 1.0

8/ Autres explications et précautions à prendre :

Vous recevez beaucoup de messages d'inconnus vous disant qu'ils ont reçu un message de votre part comportant un virus ? Vous ne connaissez pas ces gens et vous ne leur avez pas envoyé de messages. De plus, vous êtes également certain que votre machine n'est pas infectée par ce virus.

Comment cela s'explique-t-il ? Vous vole-t-on votre adresse email ? Quelqu'un usurpe-t-il votre identité ?

Il n'en est rien. Tous les derniers virus de type Worm, qui se diffusent au travers de la messagerie Outlook, modifient l'expéditeur des messages qu'ils envoient. De ce fait, sur une machine infectée, le carnet d'adresse d'Outlook est utilisé par le virus pour trouver les destinataires à qui s'auto-expédier, et il y choisit également le nom de l'expéditeur tel qu'il sera affiché. Le destinataire d'un de ces messages croit donc recevoir un message, contaminé en plus, de Monsieur X, alors qu'en fait il est parti de la machine de Monsieur Y et aucune trace ni aucun lien ne peut être fait avec le poste de Monsieur Y. Ce destinataire répond alors au message pour se plaindre de l'envoi de ce virus et c'est Monsieur X qui reçoit la plainte. Mais il n'y est pour rien.

Il n'y a pas vol d'adresse e-mail, ni usurpation volontaire d'identité, car c'est simplement dû au fonctionnement de ces virus qui masquent l'origine de leur diffusion de cette manière. Il n'est donc pas utile de répondre à tous ces messages qui vous annoncent que vous êtes infectés, il faut simplement les détruire.

Enfin, au risque de me répéter, mettez régulièrement à jour (1 fois/semaine) votre **Antivirus, **Firewall**, **Windows Update** (mises à jour critiques).**

Créez régulièrement des **Points de Restauration (vous pouvez également supprimer les anciens points de restauration pour éviter de surcharger votre disque dur).**

Faites des **sauvegardes régulières de vos dossiers sur CD ou DVD.**