# SCÉCEO SERVICES CULTURE ÉDITIONS RESSOURCES POUR L'ÉDUCATION NATIONALE CR DP. ACADÉMIE DE PARIS

# Assistance des réseaux pédagogiques

# Comment optimiser la lutte contre les Virus informatiques

# **Sommaire**

- I. Comment s'en préserver
  - a. Choisir son antivirus
  - b. Programmation de la recherche de virus
  - c. Mise à jour de l'antivirus
  - d. Mise à jour de l'O.S.
- II. Protection de la messagerie
  - a. Règles générales
  - b. Cas particulier : le logiciel Outlook Express
  - c. <u>Une parade : les notificateurs de courrier ; exemple avec les logiciels gratuit</u>

**MailWasher et NPop** 

III. Comment faire en cas d'infection?

**Adresses utiles** 

# SCÉCED SERVICES CULTURE ÉDITIONS RESSOURCES POUR L'ÉDUCATION NATIONALE CROP ACADÉMIE DE PARIS

# Assistance des réseaux pédagogiques

### I. Comment s'en préserver ?

### a. Choisir son antivirus

Il existe plusieurs technologies mais la grande majorité fonctionne sur le mode de vérification de vos fichiers avec une banque de donnée qui contient la « signature » des virus connus ; ces antivirus n'ont donc d'efficacité que si la mise à jour est faite (très) régulièrement. Si vous optez pour un a.v. payant, vérifiez bien les conditions de mise à jour : certains éditeurs d'a.v. (comme Norton) vous offrent une durée limitée de mises à jour ; à l'issue de cette licence, vous ne pourrez plus légalement télécharger les dernières signatures et votre a.v. n'aura plus aucune efficacité.

Il existe une technologie qui ne nécessite pas de mise à jour (comme Viguard); cette technologie se révèle efficace mais est rapidement contraignante pour un usage personnel. En revanche, c'est la solution la plus confortable pour équiper un gros réseau.

Certain a.v. proposent une version réseau avec automatisation de la mise à jour via un serveur. La mise en place d'une telle solution est souhaitable pour la protection d'un réseau ; néanmoins sa mise en place peut s'avérer compliquée sans une bonne connaissance du produit.

En tout état de cause, aucun a.v. n'est efficace à 100% ; on ne peut pas installer deux a.v. sur un même poste mais il est possible de doubler régulièrement la recherche de virus en utilisant un a.v. « en ligne » (comme celui proposé par <a href="www.secuser.com">www.secuser.com</a>).

REMARQUE IMPORTANTE : Depuis janvier 2003, l'académie de Paris met à disposition des établissements scolaires et des enseignants un antivirus développé par Trend Micro. Plus d'info en contactant la plateforme d'assistance au 01 40 32 34 70

### b. Programmation de la recherche de virus

Installer un a.v. sur votre machine ne vous garanti pas que celle-ci ne contient aucun virus. Seul une recherche régulière permettra d'optimiser son efficacité. Suivant l'usage qui est fait de la machine (quotidienne, beaucoup de courrier, Internet, etc.), on conviendra d'effectuer une recherche quotidienne ou hebdomadaire. La recherche de virus utilise une grande partie des ressources de la machine, préférer alors effectuer la recherche à une heure creuse.

Cette recherche peut prendre jusqu'à une heure suivant le nombre et la taille des fichiers à vérifier.

Bien regarder aussi la configuration de l'a.v.; il est préférable de vérifier tous les fichiers plutôt que seuls les exécutables (plus long mais plus sûr). La plupart des a.v. offrent comme option de réparer les virus « réparable » ; choisissez cette option même si elle n'est pas toujours efficace. En cas de détection de virus, il faudra noter son nom puis rechercher les informations le concernant afin de s'assurer de son nettoyage total.

En règle générale pensez qu'un antivirus ne sert qu'à empêcher qu'un virus s'installe sur votre machine, pas à nettoyer les virus présents. Vous n'aurez alors que des bonnes surprises.

## SERVICES CULTURE ÉDITIONS RESSOURCES POUR L'ÉDUCATION NATIONALE CR DP ACADÉMIE DE PARIS

# Assistance des réseaux pédagogiques

### c. Mise à jour de l'antivirus

Les a.v. qui comparent vos fichiers avec une banque de « signatures » de virus en sont donc efficaces que si cette banque de données est régulièrement mise à jour. La plupart des a.v. proposent un utilitaire intégré de mise à jour. Chaque éditeur propose ainsi en moyenne une mise à jour tous les 8-10 jours. Afin de n'en rater aucune, on fera une recherche de mise à jour chaque semaine. Une fois cette mise à jour effectuée, il est possible de vérifier la date de la mise à jour (pour chaque a.v. l'endroit est différent). Vérifiez bien que la mise à jour soit faite ; certains virus malin bloque cette mise à jour sans que vous ne vous en rendiez compte.

### d. Mise à jour de l'O.S. (Operating System)

Beaucoup de virus utilisent des failles dans la sécurité de votre O.S. (comme si une porte était défectueuse et qu'un intrus pouvait entrer à votre insu). Une fois la faille connue, l'éditeur de votre O.S. va essayer de corriger cet « oubli » et vous proposer une mise à jour.

Par exemple <a href="http://www.info.apple.com/support/downloads">http://www.info.apple.com/support/downloads</a> fr.html pour les O.S. Apple et <a href="Windows Update">Windows Update</a> pour les O.S. Microsoft (Windows95/98/NT/2000/XP). Il est souhaitable d'effectuer régulièrement ces mises à jour.

Pour info, certaines listes de diffusion vous informent des mises à jour majeures (comme celle de <a href="https://www.secuser.com">www.secuser.com</a>)

### II. Protection de la messagerie

### a. Règles générales

La grande majorité des virus arrivent sur votre ordinateur via les mails que vous recevez sous la forme de pièces jointes. Quelques précautions permettront de minimiser le risque d'infection.

- Lorsque vous recevez un courrier contenant une pièce jointe (ou pièce attachée) :
  - Connaissez-vous l'expéditeur ?
  - o Le corps du message a-t-il une signification réelle ?
  - o L'expéditeur vous annonce-t-il le contenu de la pièce jointe ? (expl ("ci-joint un document ...")

Si vous avez le moindre doute, renvoyez un courrier à l'expéditeur pour lui demander des précisions. Configurez votre O.S. pour afficher l'extension des fichiers dont le type est connue ; beaucoup de fichiers attachés se nomment par expl *bonjour.doc.exe* ; la plupart des O.S. masque les extensions et vous ne voyez alors que *bonjour.doc*.

De même, lorsque vous envoyez une pièce jointe à quelqu'un, décrivez au mieux ce fichier afin de lever toute ambiguïté.

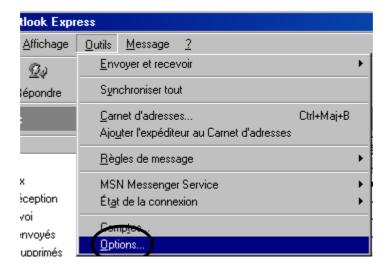


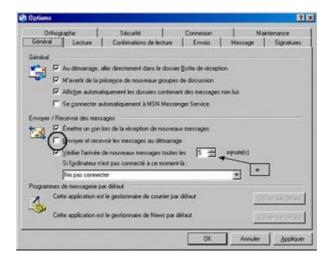
# Assistance des réseaux pédagogiques

### b. Cas particulier : le logiciel Outlook Express

Outlook Express comme tous les produits distribués par Microsoft est la cible préférée des auteurs de virus ; en l'utilisant il faut donc être doublement vigilant. Voici quelques copies d'écrans afin d'éviter les écueils les plus fréquents.

Par défaut, la configuration de Outlook Express ne protège pas au mieux votre ordinateur. Afin de ne pas risquer de diffuser à votre insu des virus, certains réglages s'imposent :

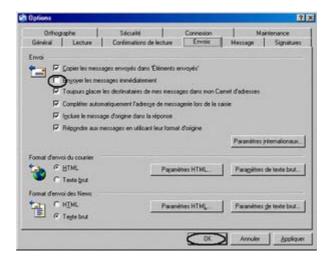




\*: Cette option est utile: laissez ouvert le logiciel et il ira chercher régulièrement le courrier.



# Assistance des réseaux pédagogiques



Avec cette configuration, lorsque vous écrivez un message et cliquez sur « Envoyer », le message est mis dans la « Boîte d'envoi ». Pour Recevoir et envoyer les message, il faudra cliquer sur l'icône « envoyer/recevoir » :



- c. Une parade : les notificateurs de courrier ; exemple des logiciels gratuits <u>MailWasher</u> et <u>NPop</u>
  - 1. Mailwasher

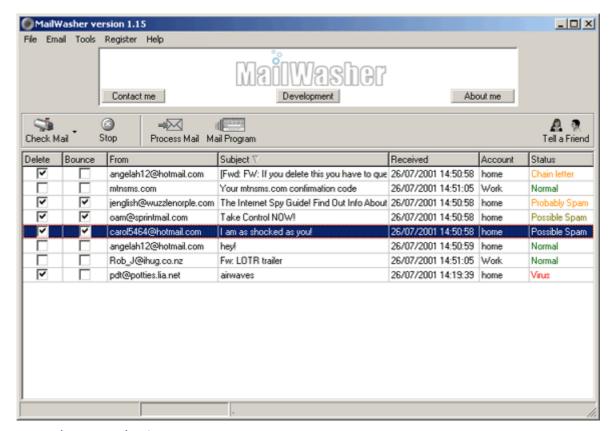
Il s'agit de la parade à tous les virus transmis par mail pour peu qu'on l'utilise correctement.

Mailwasher vous annonce:

- L'arrivée de courrier
- · Qui vous envoie ce courrier
- Si ce message contient une pièce attachée
- La taille du courrier (très utile lorsque vous avez une connexion bas débit)
- Vous pouvez aussi voir le corps du message



# Assistance des réseaux pédagogiques



Vous pouvez alors en cochant,

- Choisir de supprimer un courrier directement sans le télécharger
- Envoyer un "bounce" à l'expéditeur : en plus de le supprimer, l'expéditeur recevra un courrier du style "destinataire inconnu". Cette option est extrêmement utile pour écarter les importuns et faire barrage aux spams. Dans ce cas, l'expéditeur sera mis dans une "liste noire" et mémorisé par MailWasher.

MailWasher gère plusieurs comptes de courrier. Un utilitaire vous permet d'importer des comptes de la plupart des logiciels de courrier.

De même qu'un logiciel de courrier de base, vous pouvez le paramétrer pour rechercher automatiquement les nouveaux courriers à intervalles réguliers. vous trouverez une documentation complète sur <a href="http://archerdelaur.free.fr/utilisat.htm">http://archerdelaur.free.fr/utilisat.htm</a>

### 2. NPop

NPop est plus qu'un notificateur de courrier., c'est est un client léger de messagerie qui ne nécessite aucune installation. Sa faible taille lui permet, par exemple, d'être exécuté à partir d'une simple disquette. Vous trouverez une documentation complète de NPop ainsi que le logiciel sur <a href="ftp://ftp-pedagogique.scola.ac-paris.fr/assist\_pub/outils/web/courrier">ftp://ftp-pedagogique.scola.ac-paris.fr/assist\_pub/outils/web/courrier</a>

## SERVICES CULTURE ÉDITIONS RESSOURCES POUR L'ÉDUCATION NATIONALE CR DP. ACADÉMIE DE PARIS

# Assistance des réseaux pédagogiques

### III. Comment faire en cas d'infection?

En général, on sait qu'un virus est présent sur un poste parce qu'un antivirus vous le dit...

Si le virus est d'un type « réparable » votre AV se charge de tout. Mais ce n'est pas certain...

Beaucoup de virus modifient suffisamment d'éléments pour qu'un AV ne puisse le nettoyer. Il vous faut alors vous documenter sur le virus puis trouver un batch de nettoyage ou une procédure détaillée.

Prenons l'exemple du virus win32.blebla.b (son nom varie suivant les versions...) ; ce virus place sur la partition principale un fichier nommé sysrnj.exe puis modifie l'association de tous les fichiers exécutables pour les dévier vers ce fichier (lequel vous donnera accès de façon invisible au programme demandé). A chaque exécution, il va ronger un peu plus chaque jour votre OS (son fonctionnement en détail est flou).

Un AV va au mieux supprimer le fichier sysrnj.exe mais ne va pas ré associer les fichiers exécutables aux bons programmes ; d'où un apparent plantage de l'OS.

Il faut alors trouver sur le Web un batch qui va réparer les effets de ce virus en particulier. Dans ce cas précis on trouvera un fichier nommé « fixblebla.com » sur le Web.

En règle générale, ces utilitaires se nomment « fix\_nomduvirus.bat ou .com » (utile à savoir pour une recherche en ligne).

La plupart des éditeurs d'AV proposent des batchs de réparation.

Quel que soit le virus rencontré, le succès de son éradication repose sur sa connaissance. Il peut être utile d'appeler à l'aide sur des forums.

L'automne dernier, certains établissement parisiens ont été victime du virus réseau « nimda » ; seuls les renseignements pris sur le Web nous ont permis de le supprimer correctement.

Si vous avez un doute de la fiabilité de votre AV, n'hésitez pas à tester votre machine avec un AV « en ligne ».

### Adresses utiles :

www.secuser.com : base de connaissance, lettre de diffusion, nombreux utilitaires de réparation

fr.comp.securite.virus : forum français dédié au virus (utile pour des appels à l'aide)

http://securite.ac-creteil.fr/: info régulièrement mises à jour, liens divers.

http://www.secuser.com/outils/antivirus.htm : antivirus en ligne.

http://www.free-av.com/ : un des derniers antivirus vraiment gratuit (pour une utilisation personnelle). Soyez patient, le chargement de la page est parfois lent.

<u>http://www.framasoft.net/soft-rubrique.php3?id\_rubrique=54</u> : la page du toujours indispensable Framasoft.net dédiée aux virus.