

Bonnes pratiques¹ contre les virus

La grande majorité des virus vient par les pièces jointes des mails

Reconnaître un virus

- Si la pièce jointe est un fichier dont le nom se termine les extensions suivantes (les plus fréquentes sont en **gras**), c'est probablement un virus :

.ade, .adp, .asx, .bas, **.bat**, .chm, .cmd, .com, .cpl, .crt, **.exe**, .hlp, .hta, .inf, .ins, .isp, .js, .jse, **.lnk**, .mdb, .mde, .msc, .msi, .msp, .mst, .pcd, **.pif**, .reg, .scr, .sct, .shb, .shs, .url, .vb, .vbe, **.vbs**, .wsf, .wsh

- Si la pièce jointe se termine par les extensions suivantes c'est une archive :

.zip, .arj, .rar, .tar, .tar.gz, .tar.bz2, .tgz, .zoo, .lzh, .lha

MAIS si en regardant le contenu de l'archive on voit qu'elle contient un fichier avec l'une de ces extensions, alors c'est probablement un virus.

Que faire pour prévenir l'infection

- Ne pas activer la fonctionnalité qui existe dans les logiciels de mail d'ouvrir automatiquement les pièces jointes.
- Activer la mise à jour automatique de l'ordinateur.
- Faire des sauvegardes.
- Utiliser un firewall quand on est chez soi (entrave les chevaux de Troie).
- Avoir un antivirus à jour.

¹ Extrait d'un mémento du Certa (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques)

Réception d'un mail suspect

- Ne pas baser toute sa confiance dans l'antivirus. Même si l'antivirus ne vous alerte pas c'est peut-être un virus.
- Si on reçoit une pièce jointe suspecte :
 - Ne pas se fier à l'expéditeur (certains virus empruntent votre carnet d'adresse)
 - Ne pas cliquer sur la pièce jointe
 - Demander de l'aide
 - Détruire le message

Que faire si vous êtes contaminé ?

- Débrancher le câble réseau et le wifi de manière à ne pas risquer la propagation du virus.
- Ne pas utiliser de clé usb ou de disquette sur cette machine.
- Demander de l'aide.