

Virus et Spams : protégez-vous !

juin 2006

> Edito

Le nombre de virus et de spams augmente de façon exponentielle, empoisonnant nos usages informatiques.

Ces thèmes avaient déjà été traités dans CRI Pratique (n°2-mai 2003 et n°4-septembre 2003), mais ils prennent une telle ampleur qu'un rappel est nécessaire.

Depuis, le CRI74 a également mis en place de **nouveaux outils** pour lutter plus efficacement contre ces fléaux. Vous trouverez ici toutes les procédures à suivre pour en bénéficier. Cependant, parce que la prévention reste la meilleure arme, il est nécessaire d'acquérir certains réflexes très simples. Ce CRI Pratique n°18 vous rappelle l'essentiel de ces gestes qui peuvent **sauver votre ordinateur**.

Les virus

Un virus est un programme malveillant qui peut modifier ou détruire des fichiers, effacer les disques durs, ou encore rallonger les temps de traitement. Il peut aussi créer des vulnérabilités "cachées" qui seront exploitées par un autre processus.

Comment se protéger ?

S'il n'y a pas de système efficace à 100 %, la réunion d'outils anti-virus et d'un peu de bon sens peut résoudre bien des problèmes !

> **Installez un logiciel anti-virus** sur votre machine et mettez-le à jour régulièrement.

Le CRI74 vous propose des logiciels efficaces que vous pouvez télécharger

sur son serveur FTP (logiciels mis à disposition gratuitement par leurs éditeurs).

Pour accéder au serveur FTP du CRI74 :
> site web du CRI74 (www.cri74.org)
> rubrique Services puis services pratiques

> dans le paragraphe "Mise à disposition d'outils logiciels", accédez à l'URL du serveur FTP du CRI74 : <ftp://ftp.pub.cri74.org/>

> cliquez sur le répertoire "PUB", puis sélectionnez votre système d'exploitation. Une vaste sélection de logiciels classés par thèmes vous est proposée. Dans la rubrique **anti-virus**, faites votre choix ! (Le CRI74 recommande : **Free-Avast**).

> **Ne téléchargez jamais de programmes** d'origine douteuse qui peuvent être proposés sur des forums, des sites personnels, etc.

Si ces programmes ne contiennent pas de virus, ils peuvent contenir des spywares tout aussi nuisibles (voir CRI Pratique n°14 : http://www.thematique74.fr/rubrique.php?id_rubrique=77).

> **Créez dès maintenant, si ce n'est déjà fait, une disquette de démarrage saine** contenant un anti-virus (la plupart des anti-virus le proposent) pour une désinfection d'urgence.

> **Procédez régulièrement à des sauvegardes** du contenu important de votre disque dur. Mais attention, ne faites cette sauvegarde qu'après avoir

CRI74

Bâtiment le Salève 1 - Site d'Archamps
74160 ARCHAMPS

Tél. : +33 (0)4 50 31 56 30

Fax : +33 (0)4 50 95 38 17

Web : www.cri74.fr

Pour toute demande,
contactez votre référent :

<http://www.cri74.fr/rubrique4.html>

Le CRI74 dépend de l'AED



> Sécurité

Virus et Spams : protégez-vous !

juin 2006

vérifié l'absence de virus ! Cette sauvegarde vous sera également très utile en cas de crash de disque dur.

> Méfiez-vous de vos e-mails :

De manière générale, méfiez-vous de tout e-mail non attendu, dont l'expéditeur peut paraître connu mais qui aurait un contenu louche (texte incomplet, fichier attaché non mentionné dans le mail, adresse de l'émetteur proche d'une adresse connue mais légèrement différente, etc.).

> Méfiez-vous des annonces

concernant des virus qui ne précisent pas une adresse de site de confiance (éditeur d'anti-virus, organisme de référence...) où vérifier la véracité des propos. Il est très fréquent que des canulars ("hoax") ou autres "chaînes de l'amitié" polluent les boîtes aux lettres avec des messages alarmistes demandant de supprimer un fichier ou de propager l'information à l'ensemble du carnet d'adresses.

> Limitez les accès en écriture

sans mot de passe pour les partages réseau : beaucoup de virus ont la possibilité de se transmettre à l'ensemble du réseau à partir d'une seule machine infectée, en pénétrant sur les disques durs dont un accès est autorisé sans authentification. Avec un mot de passe pour les accès en écriture,

on évite assez simplement la propagation de ces virus.

> Attention aux pièces jointes !

N'ouvrez jamais une pièce jointe dont l'origine vous semble suspecte ou qui présente une extension "typique" signalant la présence d'un virus. Et pensez à configurer votre outil de messagerie pour qu'il n'ouvre pas automatiquement les fichiers joints.

Liste des extensions dangereuses :

.bat| .com| .exe| .pif| .vb| .lnk| .scr| .reg|
.chm| .wsh| .js| .inf| .shs| .job| .ini| .shb|
.scp| .scf| .wsc| .sct|.dll

Pour votre sécurité, le CRI74 a mis en place sur ses serveurs un **filtrage de pièces jointes**, système complémentaire aux dispositifs anti-virus traditionnels :

Il ne s'agit pas d'un anti-virus qui analyse les données arrivant sur l'ordinateur de l'utilisateur, et dont le but est de détecter un virus.

Il s'agit d'un filtre appliqué au niveau des serveurs du CRI74, triant les messages qui arrivent sur ces serveurs. Les messages suspects sont "mis de côté", parce qu'ils possèdent une pièce jointe avec une extension "typique" de virus.

Tout message qui arrive sur les serveurs du CRI74 avec l'une de ces extensions sera donc filtré.

Ces messages filtrés ne sont pas détruits, mais placés dans un répertoire spécifique (consultable avec le protocole imap).

L'utilisateur n'a ainsi pas à "charger" les messages sur son ordinateur, mais peut vérifier à tout moment les messages filtrés.

Cas particulier : le filtrage de pièces jointes de type ".zip" :

Les archives de type ".zip" sont assez courantes dans les échanges d'e-mails. Il s'agit de fichiers compressés de manière à faciliter les échanges. L'extension ".zip" n'est pas une extension "typique" de virus. Cependant, l'archive peut contenir des virus qui infiltreront l'ordinateur lorsqu'elle sera décompressée. Cette application est traitée différemment, afin de ne pas filtrer injustement des pièces jointes qui ne seraient pas des virus. C'est pourquoi les utilisateurs ont ici la possibilité d'opter pour un filtrage ou non de l'extension ".zip".

Pour bénéficier du filtrage de pièces jointes, il faut bien évidemment que vous disposiez d'un compte de messagerie au CRI74.

Pour activer ce service, voir plus loin.

Les spams

Ces courriers non sollicités à caractère commercial envahissent nos boîtes

> Sécurité

Virus et Spams : protégez-vous !

juin 2006

tes aux lettres, rallongent les durées de téléchargement des messages, nous font perdre un temps fou en traitement, bref empoisonnent nos usages informatiques !

Comment protéger sa boîte ?

> **Ne communiquez jamais votre adresse** sur des sites de commerce électronique, sur des listes de diffusion, sur des forums, sur ses pages personnelles, etc. En effet, des "robots" sont programmés pour scruter l'ensemble des sites web afin de récolter toutes les adresses e-mail.

Si vous voulez acheter en ligne ou participer à des forums, il est préférable d'utiliser une adresse créée à cette fin. C'est donc cette adresse qui sera polluée, mais vos adresses personnelles ou professionnelles seront épargnées.

> Utilisez un outil anti-spam :

Le CRI74 vous propose des logiciels efficaces que vous pouvez télécharger sur son serveur FTP (logiciels mis à disposition gratuitement par leurs éditeurs).

Pour accéder au serveur FTP du CRI74 :

> site web du CRI74 (www.cri74.org)
> rubrique Services puis services pratiques

> dans le paragraphe "Mise à disposition d'outils logiciels",

accédez à l'URL du serveur FTP du CRI74 : <ftp://ftp.pub.cri74.org/>

> cliquez sur le répertoire PUB, puis sélectionnez votre système d'exploitation.

Une vaste sélection de logiciels classés par thèmes vous est proposée. Dans la rubrique **anti-spam**, faites votre choix ! (Le CRI74 recommande : **Spamihilator**).

> Adoptez Thunderbird :

Thunderbird est un outil de messagerie de la famille Mozilla. Il est libre. Très léger, très pratique, cet outil vous propose notamment une fonction anti-spam intelligente : chaque e-mail reçu est analysé par des filtres. À chaque fois que vous marquez un message comme indésirable, cette décision est répercutée dans l'analyse statistique globale du courrier entrant, afin d'améliorer la détection des messages publicitaires.

Pour télécharger Thunderbird :

> site web du CRI74 (www.cri74.org)
> rubrique Services puis services pratiques

> dans le paragraphe "Mise à disposition d'outils logiciels", accédez à l'URL du serveur FTP du CRI74 : <ftp://ftp.pub.cri74.org/>

> cliquez sur le répertoire PUB, puis sélectionnez votre système d'exploitation.

Une vaste sélection de logiciels clas-

sés par thèmes vous est proposée. Dans la rubrique **mailclient**, choisissez **Mozilla Thunderbird**.

ou sur le site officiel :

<http://www.mozilla-europe.org/fr/products/thunderbird/>

Pour votre sécurité, le CRI74 a mis en place un **système expérimental complémentaire aux dispositifs anti-spam traditionnels** :

Ce système analyse finement les e-mails entrant. Des points sont attribués à l'e-mail selon des caractéristiques bien précises. Le résultat de ces tests permettra au système de repérer les spams.

Les pourriels ainsi démasqués ne sont pas détruits, mais placés dans un répertoire spécifique consultable avec le protocole imap.

Grâce à ce protocole, l'utilisateur ne "charge" pas les messages sur sa machine (pas de perte de temps), mais peut vérifier à tout moment la précision du filtrage.

Pour bénéficier du filtrage de spams, il faut bien évidemment que vous disposiez d'un compte de messagerie au CRI74.

Comment **activer** le service de filtrage de spams et le filtrage de pièces jointes comportant des virus mis en place par le CRI74 ?

Le CRI74 ne peut pas activer ce service

> Sécurité

Virus et Spams : protégez-vous !

juin 2006

à votre place et sans votre autorisation. Vous devrez donc lire et accepter les conditions d'utilisation afin de bénéficier de ce service.

Le service de filtrage ne s'applique qu'aux boîtes aux lettres électroniques hébergées au CRI74.

Pour accéder au service, vous devez aller à cette URL :

<http://www.cri74.org/rubrique43.html>

Cette rubrique correspond aux accès restreints (réservés aux utilisateurs du CRI74). Vous devez vous authentifier en fonction de la nature de votre structure (établissement scolaire = edres74, etc.). Le login et le password demandés figurent sur la feuille de compte qui vous a été remise lors de la création de votre compte (il ne s'agit pas du mot de passe "messagerie" mais du mot de passe "web restreint").

Ces informations sont confidentielles : ne les laissez pas à la portée d'autrui !

Après vous être identifié, choisissez

> **ACTIVATION/DESACTIVATION DES MECHANISMES DE FILTRAGE SUR LE COURRIER ELECTRONIQUE**

Vous accédez ainsi à l'interface de filtrage. La première page vous indique si votre boîte aux lettres bénéficie ou non du service de filtrage. Si votre boîte ne bénéficie pas encore de ce service, vous devez l'activer en acceptant les conditions générales d'utilisation : sui-

vez le lien qui vous renvoie sur elles et cochez la case.

Une documentation et une FAQ vous permettront de mieux comprendre le procédé mis en place.

Pour toute question : merci de vous adresser à votre référent dont vous trouverez les coordonnées ici :
<http://www.cri74.org/rubrique4.html>

Note :

Certains e-mails bénéficient déjà de ce service de manière expérimentale ; d'autres en bénéficient également déjà grâce à une autorisation de leur institution (certaines boîtes éducation publique 1er degré notamment).

Certains comptes ne peuvent cependant pas bénéficier de ce service :

> Les comptes mail sur les Ping00 v2 et v3.

> Les messageries électroniques qui ne sont pas gérées par le CRI74 même si leur nom de domaine est bien hébergé par le CRI74. Ces comptes ont en effet leur propre serveur de messagerie. Dans ce cas, les e-mails ne font que transiter par les serveurs du CRI74 et ne peuvent pas bénéficier du service.

> Les comptes e-mail qui sont gérés sur les serveurs du CRI74 mais qui renvoyés à la demande de l'utilisateur sur une boîte e-mail externe (de type Free, Wanadoo, etc.). En effet, l'analyse des e-mails par le CRI74 ne se fait qu'à la délivrance finale du message. Cette délivrance, dans ce cas précis, n'a donc pas lieu puisque l'e-mail est "forwardé" sur une autre boîte.

> Conclusion

Ne vous laissez pas décourager par la prolifération de ces e-mails, mais adoptez les bons outils et les bons réflexes.

Vos référents sont à votre disposition pour vous aider à résoudre ces problèmes, n'hésitez pas à les solliciter !

Vous trouverez leurs coordonnées ici :

<http://www.cri74.org/rubrique4.html>

Merci de respecter la procédure qui figure à cette adresse. Les demandes adressées au mauvais référent ne pourront pas être traitées.

Retrouvez tous les CRI Pratique

sur :

www.thematic74.fr