



Les virus et le spam ce qu'il faut savoir

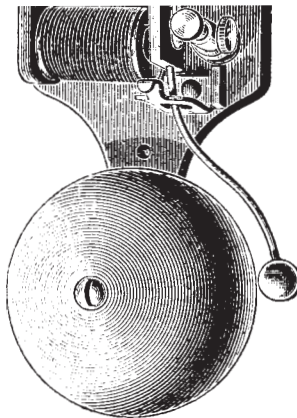


SOPHOS

Les virus et le spam

ce qu'il faut savoir

Si vous êtes un administrateur réseau, si vous utilisez un ordinateur au bureau ou si simplement vous lisez des courriels, ce livret est pour vous. Nous vous exposons en des termes simples les faits concernant les virus informatiques et le spam.



Sophos est l'un des principaux éditeurs mondiaux de logiciels antivirus et anti-spam, protégeant plus de 25 millions d'utilisateurs professionnels dans le monde. Pour en savoir plus sur la gamme complète de solutions Sophos pour se protéger contre le spam et les virus et pour appliquer dans l'entreprise une politique de sécurité de la messagerie, consultez notre site Web à l'adresse www.sophos.fr



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Copyright © 2001, 2003, 2004 par Sophos Plc

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sans le consentement préalable écrit du propriétaire du copyright.

Sauf indication contraire, il est supposé que tout nom est une marque commerciale. Sophos est une marque déposée de Sophos Plc.

ISBN 0-9538336-3-1

Site Web : www.sophos.fr

Table des matières

Virus, chevaux de Troie et vers 5

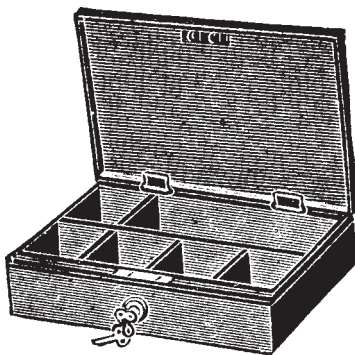
Le spam 27

Canulars et escroqueries 41

Astuces pour une informatique sécurisée 49

Glossaire 53

Index 65



Virus



Spam



Canulars



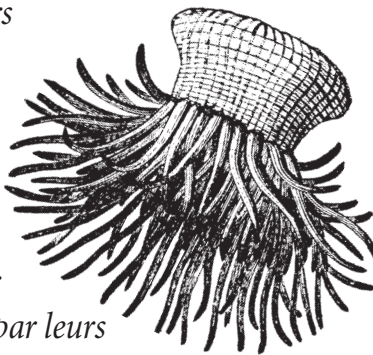
Sécurité



Références

Virus, chevaux de Troie et vers

Au milieu des années 1980, deux frères pakistanais s'aperçurent que des personnes pirataient leurs logiciels. Ils réagirent en écrivant le premier virus informatique, programme plaçant sa propre réplique et un message de copyright sur chaque disquette copiée par leurs clients. De cet événement simple a émergé toute une contre-culture du virus. Aujourd'hui, les nouveaux virus peuvent balayer la planète en quelques minutes et corrompre des données, ralentir les réseaux ou porter atteinte à votre réputation.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Qu'est-ce qu'un virus ?

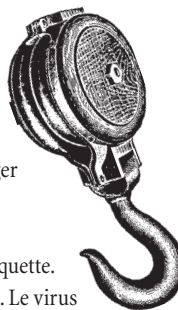
Un virus ou ver est un programme informatique qui peut se propager à travers les ordinateurs et les réseaux en créant ses propres copies, et cela, généralement à l'insu des utilisateurs.

Les virus peuvent avoir des effets néfastes : affichage de messages agaçants, subtilisation de données ou transfert du contrôle de votre ordinateur à d'autres utilisateurs.

Comment le virus infecte-t-il l'ordinateur ?

Pour infecter votre ordinateur, un programme de virus doit au préalable être exécuté. Les virus ont des moyens pour s'assurer que cela arrive. Ils peuvent se fixer sur d'autres programmes ou se dissimuler au sein d'un code de programmation qui s'exécute automatiquement à l'ouverture de certains types de fichiers. Ils peuvent aussi exploiter des failles de sécurité présentes sur le système d'exploitation de votre ordinateur et se propager automatiquement.

Le fichier infecté peut provenir d'une pièce jointe de courriel, du Web lors d'un téléchargement ou d'une disquette. Dès que le fichier est lancé, le code du virus est exécuté. Le virus peut ensuite se copier sur d'autres fichiers ou disquettes et modifier votre ordinateur.



Chevaux de Troie

En se faisant passer pour des logiciels légitimes, les chevaux de Troie sont des programmes qui exécutent des fonctions cachées néfastes.

Par exemple, *DLoader-L* arrive dans une pièce jointe de courriel et prétend être une mise à jour urgente de Microsoft pour Windows XP. Si vous l'exécutez, il télécharge un programme qui utilise votre ordinateur pour se connecter à certains sites Web dans le but de les surcharger (cela s'appelle une attaque par déni de service).



Les chevaux de Troie ne peuvent pas se propager aussi rapidement que les virus car ils ne font pas de copie d'eux-mêmes. Par contre, ils fonctionnent désormais souvent en étroite collaboration avec des virus. En effet, les virus peuvent télécharger des chevaux de Troie qui enregistrent des frappes de touches ou subtilisent des informations. D'autre part, certains chevaux de Troie sont utilisés par des virus pour infecter un ordinateur.

Vers

Les vers sont semblables aux virus mais ne nécessitent pas de programme ou de document porteur.

Les vers ne font que créer leur réplique exacte et utilisent les transmissions entre ordinateurs pour se propager (voir la section "Vers Internet").

De nombreux virus, tels *MyDoom* ou *Bagle*, se comportent comme des vers et utilisent la messagerie pour s'expédier eux-mêmes.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité

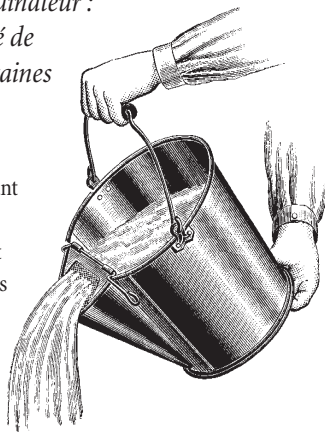


Références

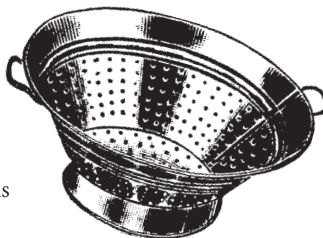
De quoi sont capables les virus ?

Auparavant, les virus faisaient des farces ou interrompaient le fonctionnement de l'ordinateur : maintenant, ils compromettent la sécurité de façon beaucoup plus insidieuse. Voici certaines des actions dont sont capables les virus.

- **Ralentir la messagerie.** Les virus se propageant par courriel comme *Sobig* peuvent générer un trafic de messagerie si important que cela peut entraîner le ralentissement ou l'arrêt brutal des serveurs. Même si cela ne se produit pas, l'entreprise peut tout de même réagir en éteignant les serveurs.
- **Subtiliser des données confidentielles.** Le ver *Bugbear-D* enregistre les saisies clavier de l'utilisateur, y compris les mots de passe, et donne à l'auteur du virus l'accès à ces données.
- **Utiliser votre ordinateur pour attaquer les sites Web.** *MyDoom* utilisait des ordinateurs infectés pour inonder de données le site Web de la société informatique SCO, rendant ainsi le site inutilisable (une attaque par déni de service).



- **Permettre à d'autres utilisateurs de pirater votre ordinateur.** Certains virus placent des "Chevaux de Troie de porte dérobée" sur l'ordinateur, ce qui permet à l'auteur de virus de se connecter à votre ordinateur et de l'utiliser comme bon lui semble.
- **Corrompre des données.** Le virus *Compatable* effectue des changements dans les données des tableaux Excel.
- **Effacer des données.** Le ver *Sircam* peut tenter un jour donné de supprimer ou d'écraser le disque dur.
- **Désactiver des matériels.** *CIH*, plus connu sous le nom de *Chernobyl*, entreprend d'écraser le BIOS le 26 avril, rendant de ce fait la machine inutilisable.
- **Faire des farces.** Le ver *Netsky-D* fait émettre à l'ordinateur des signaux sonores sporadiques pendant toute une matinée.
- **Afficher un message.** *Cone-F* affiche un message politique s'il s'agit du mois de mai.
- **Nuire à la crédibilité.** Si un virus s'expédie de lui-même de votre ordinateur vers ceux de vos clients ou de vos partenaires commerciaux, ces derniers pourront refuser de collaborer avec vous ou souhaiteront obtenir des compensations.
- **Mettre dans l'embarras.** Par exemple, *PolyPost* place vos documents et votre nom sur des forums à caractère sexuel.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Les risques d'infection virale ?

Les virus peuvent atteindre votre ordinateur via tous les moyens indiqués ci-dessous. De plus amples détails sont disponibles dans les pages qui suivent.

Programmes et documents

Les programmes et les documents peuvent être infectés par des virus. Lorsque vous les partagez avec d'autres utilisateurs en les plaçant sur votre réseau ou Intranet ou en les envoyant, l'infection peut se propager.

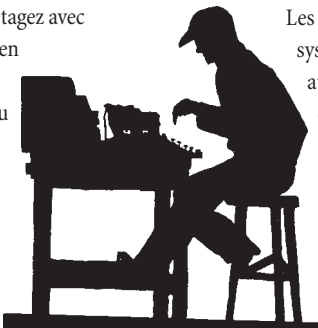
Courriel

Le courriel peut inclure des pièces jointes infectées. Si vous cliquez deux fois sur une pièce jointe infectée, vous courez le risque d'infecter votre machine. Certains courriels contiennent des scripts malveillants qui s'exécutent dès que vous voyez un aperçu du courriel ou lisez son corps de texte.

Internet

Vous pouvez télécharger des programmes ou des documents infectés.

Les failles de sécurité de votre système d'exploitation peuvent aussi permettre aux virus d'infecter votre ordinateur via la connexion Internet, cela sans que vous ayez à intervenir.



CD-ROM et disquettes

Les disquettes peuvent avoir un virus dans le secteur de démarrage. Elles peuvent aussi contenir des programmes ou des documents infectés. Les CD-ROM peuvent aussi contenir des éléments infectés.

Quels sont les fichiers infectables ?

Les virus peuvent être rattachés à tout code fonctionnant sur votre ordinateur : programmes, documents ou fichiers lançant le système d'exploitation.

Programmes

Certains virus infectent les programmes. Lorsque vous démarrez le programme infecté, le virus est lancé en premier. Ce type de virus a fait son apparition au tout début de l'histoire des virus mais constitue toujours une menace car Internet facilite la distribution des programmes.



Documents

Les logiciels de traitement de texte ou les tableurs utilisent souvent des “macros” pour automatiser les tâches. Certains virus prennent la forme d’une macro pouvant se propager d’un document à un autre. Si vous ouvrez un document qui contient le virus, il se copie dans les fichiers de démarrage de l’application et infecte les autres documents que vous ouvrez avec cette application.

Secteurs de démarrage

Lorsque vous mettez votre ordinateur en route, il accède à une partie du disque appelée le “secteur de démarrage” et exécute un programme qui lance le système d’exploitation. Les premiers virus remplaçaient ce secteur de démarrage par leur propre version modifiée. Si l’utilisateur démarrait l’ordinateur à partir d’un disque infecté, le virus s’activait.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



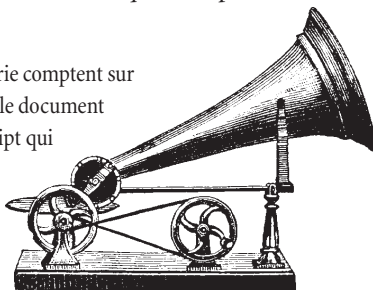
Références

Virus de messagerie

La plupart des virus les plus prolifiques sont dits “de messagerie” : ils se distribuent automatiquement par courriel.

En général, les virus de messagerie comptent sur l'utilisateur pour qu'il clique sur le document joint. Cette action exécute un script qui peut réacheminer les documents infectés vers d'autres personnes. Par exemple, le virus *Netsky* recherche sur l'ordinateur les fichiers pouvant contenir des adresses électroniques (comme des fichiers EML ou HTML), puis utilise le logiciel de messagerie présent sur l'ordinateur pour s'envoyer à ces adresses. Certains virus, comme *Sobig-F*, n'ont même pas besoin de ce logiciel de messagerie puisqu'ils ont leur propre “moteur SMTP” pour envoyer des courriels.

Les virus de messagerie peuvent compromettre la sécurité de votre ordinateur ou subtiliser des données, mais leur effet le plus répandu reste une création excessive de trafic de messagerie et l'arrêt brutal des serveurs.



Pièces jointes de courriels

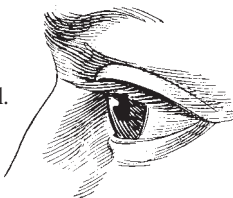
Toute pièce jointe que vous recevez par courriel peut porter un virus ; le lancement d'une telle pièce jointe peut infecter votre ordinateur.

Même une pièce jointe qui semble être un fichier sain avec, par exemple, une extension .txt peut constituer une menace. En effet, ce fichier peut être un script VBS malveillant dont le véritable type (.vbs) est caché.

Puis-je recevoir un virus rien qu'en lisant un courriel ?

Il n'est pas nécessaire d'ouvrir une pièce jointe pour être infecté par courriel. Visualiser son courriel constitue déjà un risque.

Certains virus, comme *Kakworm* et *Bubbleboy*, peuvent infecter l'utilisateur à la lecture d'un courriel. Ressemblant à n'importe quel autre message, ils contiennent un script caché qui s'exécute dès que vous



ouvrez le courriel et même lorsque vous le consultez dans le volet de prévisualisation (dans la mesure où vous utilisez Outlook avec la version correcte d'Internet Explorer). Ce script peut changer les paramètres système et envoyer par courriel le virus à d'autres utilisateurs.

Microsoft publie des correctifs qui éliminent cette faille de sécurité ainsi que d'autres de même type. Pour en savoir plus sur les correctifs dont vous avez besoin, consultez le site windowsupdate.microsoft.com. Pour vous tenir informé des correctifs à paraître, vous pouvez vous inscrire à une liste de diffusion à l'adresse www.microsoft.com/technet/security/bulletin/notify.asp



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

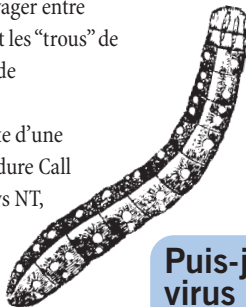
Vers Internet

Sans même ouvrir de courriel suspect, vous courez un risque chaque fois que vous êtes connecté à Internet.

Les vers Internet parviennent à voyager entre ordinateurs connectés en exploitant les “trous” de sécurité du système d’exploitation de l’ordinateur.

Le ver *Blaster*, par exemple, profite d’une faille dans le service Remote Procedure Call exécuté sur les ordinateurs Windows NT, 2000 et XP pour envoyer une réplique de lui-même sur un autre ordinateur. Au fur et à mesure que le ver se propage, il crée beaucoup de trafic sur Internet et provoque le ralentissement des communications ou l’arrêt brutal des ordinateurs. Ce ver en particulier utilise par ailleurs l’ordinateur pour inonder de données le site Web de Microsoft avec comme objectif de rendre le site inaccessible.

Microsoft (ainsi que d’autres distributeurs de systèmes d’exploitation) publient des correctifs contre les failles de sécurité de leurs logiciels. Mettez régulièrement à jour votre ordinateur en visitant le site Web du distributeur.



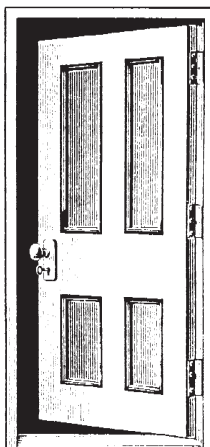
Puis-je recevoir un virus provenant d’un site Web ?

Les pages Web sont écrites en langage HTML (Hypertext Markup Language). Ce langage ne peut pas lui-même transporter de virus mais peut appeler des programmes ou des fichiers qui eux en transportent. Vous ne pouvez pas être infecté en consultant une page HTML à moins qu’il n’y ait sur votre ordinateur une faille de sécurité permettant l’exécution d’un programme qui lui vous infectera.

Chevaux de Troie de porte dérobée

Un cheval de Troie de porte dérobée est un programme qui permet à une personne de prendre le contrôle de l'ordinateur d'une autre personne via Internet.

A l'instar de n'importe quel cheval de Troie, le cheval de Troie de porte dérobée peut apparaître comme un logiciel légitime pour que l'utilisateur puisse l'exécuter. Aujourd'hui, et cela est de plus en plus fréquent, un virus peut placer un cheval de Troie de porte dérobée sur un ordinateur. Une fois que le cheval de Troie est exécuté, il s'ajoute à la routine de lancement de l'ordinateur. Il peut alors surveiller l'ordinateur jusqu'à ce que l'utilisateur soit connecté à Internet. Une fois l'ordinateur en ligne, la personne qui a envoyé le cheval de Troie peut exécuter des programmes sur l'ordinateur infecté, accéder à des fichiers personnels, modifier et charger des fichiers, traquer les saisies clavier de l'utilisateur ou envoyer un courriel de spam. Les chevaux de Troie de porte dérobée les plus connus sont *Subseven*, *BackOrifice* et *Graybird*, lequel fut déguisé en correctif pour le fameux ver *Blaster*.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Logiciel espion (spyware)

Le logiciel espion ou spyware est un logiciel qui permet aux publicitaires de rassembler des informations sur les habitudes des utilisateurs de PC.

Les logiciels espions ne sont pas des virus (vous ne pouvez pas les propager sur d'autres ordinateurs), mais ils peuvent avoir des effets indésirables.

Des logiciels espions peuvent s'installer sur votre ordinateur lorsque vous visitez certains sites Web. Un message contextuel peut vous inviter à télécharger un logiciel utilitaire dont vous pouvez "avoir besoin" ou un logiciel peut à votre insu se télécharger automatiquement.

Le logiciel espion fonctionne alors sur l'ordinateur, suit à la trace vos actions (par exemple, les visites sur les sites Web) et en fait un compte-rendu destiné par exemple à un annonceur. Il peut aussi changer la page d'accueil qui apparaît lorsque vous lancez votre navigateur Internet et utiliser un modem à composition automatique pour appeler des numéros de téléphone de type 0900 (tarifs surtaxés).

Le logiciel espion utilise la capacité mémoire et de traitement, et peut ralentir l'ordinateur ou l'arrêter brutalement.

Il existe des logiciels qui permettent de détecter les programmes espions connus et de les supprimer.



Cookies

Lorsque vous visitez un site Web, il peut placer sur l'ordinateur un petit ensemble de données appelé un "cookie". Le site se rappelle ainsi des détails vous concernant et possède une trace de vos visites.

Les cookies ne constituent pas une menace pour vos données. En revanche, ils menacent votre confidentialité. Si vous préférez rester anonyme, utilisez les paramètres de sécurité de votre navigateur pour désactiver les cookies.

Peut-on recevoir un virus sur un téléphone mobile ?

Les mobiles peuvent être infectés par des vers qui se propagent via le réseau de téléphonie mobile bien qu'à l'heure où nous écrivons, les risques semblent limités.

En 2004, le premier ver de téléphone mobile est écrit. Le ver *Cabir-A* affecte les téléphones qui utilisent le système d'exploitation Symbian et se transmet sous la forme d'un fichier de jeu téléphonique (un fichier SIS). Si vous lancez le fichier, un message apparaît à l'écran et le ver est exécuté chaque fois que vous mettez par la suite le téléphone en route. *Cabir-A* recherche dans son voisinage immédiat d'autres téléphones portables dotés de la technologie Bluetooth et s'envoie au premier qu'il trouve. Ce ver démontre qu'une infection est possible, mais il n'a pas fait l'objet d'une diffusion sur un réseau public.

Il existe aussi des virus conventionnels qui envoient des messages aux téléphones portables. Par exemple, *Timo-A* utilise les modems des utilisateurs pour envoyer des messages textuels (SMS) à des numéros de mobiles sélectionnés, mais dans ce cas-là, le virus ne peut pas infecter ou nuire au téléphone mobile.

Pour le moment, les téléphones mobiles courent peu de risques car ils utilisent des systèmes d'exploitation différents et car les caractéristiques des logiciels et des périphériques changent très rapidement.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Court-on des risques avec Bluetooth ?

La technologie Bluetooth pour téléphones portables, ordinateurs et autres systèmes peut être la porte ouverte aux virus, à la violation de la sécurité ou aux canulars.

Cette technologie permet aux ordinateurs, aux téléphones mobiles et même aux magnétoscopes ou aux réfrigérateurs de localiser les appareils les plus proches et d'établir de manière transparente des liens avec ceux-ci.

Bluetooth a déjà été exploité par un ver de téléphone mobile qui l'utilise pour rechercher des téléphones se trouvant à proximité auxquels il peut se réexpédier.

Les technologies basées sur Bluetooth comme Jini permettent également un contrôle à distance des services. Bluetooth et Jini sont conçues de manière à ce que seul le code fiable puisse exécuter des opérations sensibles ; cependant, ces technologies ouvrent de nouvelles possibilités pour du code malveillant d'interférer avec les services.

Les téléphones activés par Bluetooth peuvent aussi servir à localiser à proximité d'autres utilisateurs de téléphones et à leur envoyer des messages inattendus et parfois offensants.

Pour vous protéger contre toutes sortes de menaces Bluetooth, qu'il s'agisse de programmes malveillants ou de messages non désirés, désactivez sur votre téléphone le paramètre Bluetooth "visible pour les autres".



Peut-on recevoir un virus sur un palmtop ?

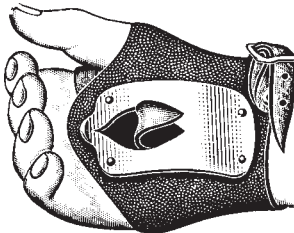
Bien que les palmtops ou les assistants électroniques constituent de nouvelles opportunités pour les virus, les auteurs de virus leur ont jusqu'à présent manifesté peu d'intérêt.

Les palmtops ou les assistants électroniques exécutent des systèmes d'exploitation particuliers tels que Palm et Microsoft PocketPC. Ces derniers sont vulnérables au code malveillant, mais jusqu'à présent les risques n'ont pas été très sérieux.

Il existe seulement un virus écrit pour Palm, ainsi qu'un cheval de Troie, mais ni l'un ni l'autre ne semblent avoir été diffusés.

Les auteurs de virus préfèrent cibler les postes de travail, peut-être parce qu'ils sont plus populaires et permettent aux virus de se propager rapidement par courriel et par Internet.

Actuellement, le véritable risque est que votre palmtop serve de porteur. Lorsque vous le reliez à un PC à domicile ou au bureau pour synchroniser les données, un virus inoffensif sur le palmtop peut se propager sur le PC où il peut être nuisible. Pour éviter cela, suivez les "Conseils pour une informatique sécurisée" et assurez-vous qu'un logiciel antivirus est installé sur votre ordinateur.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Logiciel antivirus

Le logiciel antivirus peut détecter les virus, empêcher l'accès aux fichiers infectés et souvent éliminer l'infection.

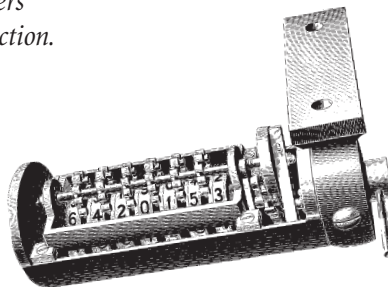
Scanneur de virus

Le scanneur de virus détecte et procède la plupart du temps à la désinfection des virus qu'il connaît. Il est de loin la forme la plus populaire de logiciel antivirus et doit être régulièrement mis à jour pour reconnaître les nouveaux virus.

Le scanneur peut être sur accès ou à la demande. De nombreuses solutions offrent les deux.

Le *scanneur sur accès* reste actif sur votre machine chaque fois que vous l'utilisez. Il vérifie automatiquement les fichiers au fur et à mesure que vous essayez de les ouvrir ou de les exécuter et peut vous empêcher d'utiliser des fichiers infectés.

Le *scanneur à la demande* vous permet de lancer ou de planifier un contrôle de fichiers ou de lecteurs spécifiques.



Logiciel heuristique

Le logiciel heuristique tente de détecter les virus connus comme inconnus en utilisant les règles générales de reconnaissance des virus.

C'est un logiciel non basé sur des mises à jour fréquentes. En revanche, il peut aussi faire l'objet de fausses alertes.

Qui écrit les virus ?

Si votre ordinateur ou votre réseau est touché par un virus, votre première réaction, en dehors de quelques jurons, est de vous demander pourquoi des individus écrivent des virus.

Les auteurs de virus désirent parfois diffuser un message politique ou nuire à une entreprise de laquelle ils ont une opinion défavorable (de nombreux virus et vers ont par exemple critiqué ou ciblé Microsoft). Ils peuvent aussi pénétrer de force sur les ordinateurs d'autres utilisateurs ou recueillir des adresses électroniques, puis vendre ces informations aux spammeurs.

Les auteurs de virus sont plus souvent motivés par la notoriété que leurs exploits peut leur apporter.

Les auteurs de virus sont, en général, des hommes, célibataires et âgés de moins de 25 ans. L'estime qu'ils ont d'eux-mêmes est fortement liée à la reconnaissance de leurs pairs, ou tout au moins d'une petite communauté de fanas d'informatique. L'écriture de virus, comme le graffiti, est une sorte de performance qui permet à son auteur d'accéder à un certain statut.

Par ailleurs, les virus donnent à leurs auteurs des pouvoirs virtuels qu'ils ne peuvent avoir dans le monde réel. C'est sans doute pour cette raison que les auteurs de virus choisissent des noms inspirés de la musique Heavy Metal ou de la littérature fantastique, lesquelles se nourrissent aussi des illusions de prouesse et de puissance.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Rappel historique des virus

Années 50

Les laboratoires Bell mettent au point un jeu expérimental où les joueurs utilisent des programmes malveillants pour attaquer leurs ordinateurs respectifs.

1975

L'auteur de science-fiction John Brunner imagine un "ver" informatique qui se répandrait à travers les réseaux.

1984

Fred Cohen introduit le terme "virus informatique" dans une thèse consacrée à ces programmes.

1986

Le premier virus informatique, *Brain*, serait écrit par deux frères pakistanais.

1987

Le ver *Christmas tree* paralyse le réseau mondial d'IBM.

1988

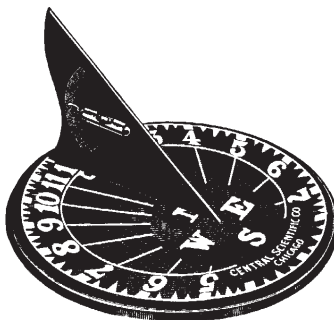
Le ver *Internet* se propage à travers le réseau internet américain DARPA.

1992

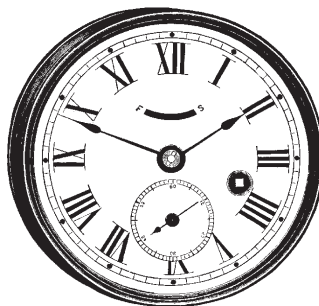
Même si très peu d'ordinateurs sont infectés, le virus *Michelangelo* provoque une panique mondiale.

1994

Apparition de *Good Times*, premier grand canular de virus.



- 1995** Apparition de *Concept*, premier virus de document.
- 1998** *CIH* ou *Chernobyl* devient le premier virus à paralyser le matériel informatique.
- 1999** Propagation de *Melissa*, un virus qui s'expédie lui-même par courriel. Apparition de *Bubbleboy*, le premier virus à infecter un ordinateur lorsqu'on visualise un courriel.
- 2000** *Love Bug* devient à ce jour le virus de messagerie le plus efficace. Le premier virus apparaît pour le système d'exploitation Palm, mais aucun utilisateur n'est infecté.
- 2001** Un virus prétendant contenir des photos de la joueuse de tennis Anna Kournikova infecte des centaines de milliers d'ordinateurs dans le monde.
- 2002** David L Smith, l'auteur de *Melissa*, est condamné à 20 mois de prison par les tribunaux américains.
- 2003** Le ver *Blaster* se propage sur Internet en profitant d'une faille de sécurité dans les logiciels Microsoft. Avec le virus de messagerie *Sobig*, ils font du mois d'août 2003 l'une des périodes les plus difficiles en matière d'incidents viraux.
- 2004** Les créateurs de la série de vers *Netsky* et *Bagle* se font concurrence pour savoir qui fera le plus de dégâts.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

L'écriture de virus est-elle répréhensible ?

Il va de soi pour la plupart des gens que les virus sont nuisibles, mais est-ce forcément vrai ?

De nombreux virus sont “inoffensifs” ou revêtent l'apparence d'une blague. D'autres nous alertent sur des failles de sécurité existantes dans certains logiciels. Certains soutiennent que les virus pourraient même s'avérer utiles, en prodiguant par exemple des correctifs pour les bogues. Malheureusement, l'innocuité supposée des virus ne résiste pas à un examen plus approfondi.

Premièrement, les virus opèrent des changements sur les ordinateurs sans le consentement de l'utilisateur. Que l'intention soit bonne ou mauvaise, cette activité est amoral et illégale dans de nombreux pays. Comme il ne viendrait à l'idée de personne d'emprunter la voiture de quelqu'un sans lui en demander l'autorisation, on ne doit pas s'immiscer dans l'ordinateur d'autrui.

Deuxièmement, le virus ne réalise pas toujours ce qui est prévu par l'auteur. Si un virus est mal programmé, il peut causer des dégâts imprévisibles. Il a beau être inoffensif sur un système, il peut très bien être nuisible sur d'autres.

Troisièmement, les virus se propagent sans faire de distinction : l'auteur n'a aucun contrôle sur les destinataires de son virus.

Les virus de démonstration

Parfois, des virus sont écrits pour prouver qu'on peut toujours en créer des nouveaux. On les appelle des virus de démonstration (ou “*proof-of-concept*”). Ils sont généralement dépourvus d'effets secondaires et n'ont pas vocation à être diffusés sur d'autres ordinateurs.

Recherche virale ?

Les auteurs de virus aiment clamer qu'ils font de la recherche. Pourtant, les virus sont souvent des programmes de piètre qualité, lancés à l'aveuglette vers des utilisateurs pris au dépourvu, et il n'existe aucun moyen d'en analyser les résultats. Ce n'est guère ce qu'on peut appeler de la recherche.

Prévention des virus

Des mesures simples existent pour éviter l'infection ou se débarrasser de virus en cas d'infection. Pour plus de détails, consultez le chapitre intitulé "Conseils pour une informatique sécurisée".

Sensibilisez les utilisateurs aux risques qu'ils encourent

Avertissez votre entourage qu'il s'expose à des risques en cas d'ouverture de pièces jointes à des courriels, de téléchargement de fichiers depuis des sites Web ou d'échange de disquettes.

Installez un logiciel antivirus et mettez-le à jour régulièrement

Les programmes antivirus peuvent détecter et souvent supprimer les virus par désinfection. Si le logiciel inclut la vérification virale sur accès, n'hésitez pas à l'utiliser.

Utilisez des correctifs logiciels contre les failles de sécurité

Soyez toujours à l'affût des "correctifs" correspondant à votre système d'exploitation. Ils permettent souvent de colmater les failles qui vous fragilisent vis-à-vis des virus.

Utilisez des pare-feu

Un pare-feu peut empêcher un accès non autorisé à votre réseau, mais aussi empêcher les virus d'expédier des informations.

Conservez des sauvegardes de toutes vos données

Conservez des sauvegardes de toutes vos données et logiciels, y compris des systèmes d'exploitation. Si vous êtes touché par un virus, vous pourrez ainsi remplacer vos fichiers et programmes par des copies saines.



Virus



Spam



Canulars



Sécurité

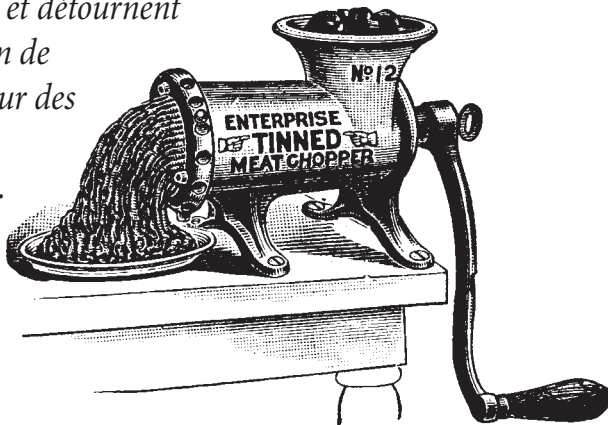


Références



Le spam

Il vous est déjà très certainement arrivé de recevoir des courriels vous proposant des médicaments sans prescription, des prêts ou des méthodes d'enrichissement personnel rapide, parfois habilement déguisés en courriels personnels. Représentant plus de la moitié du trafic de courriels envoyés dans le monde, ces messages "spam" obstruent les boîtes de réception et détournent l'attention de l'utilisateur des messages essentiels.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

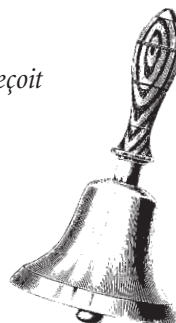
Qu'est-ce qu'un spam ?

Le spam est un courriel commercial non sollicité, l'équivalent électronique de la "publicité" que l'on reçoit dans sa boîte aux lettres.

Les spams les plus répandus concernent :

- la prescription de médicaments qui agrandissent ou perfectionnent des parties de votre corps, des remèdes à base d'herbes ou des médicaments pour vous aider à perdre du poids
- des méthodes pour s'enrichir rapidement
- des services financiers comme des offres d'emprunts à taux préférentiel ou des méthodes de réduction des dettes
- des qualifications comme un diplôme universitaire ou un titre professionnel à acheter
- des jeux d'argent en ligne
- des logiciels à prix défiant toute concurrence ou piratés.

Le spam apparaît parfois déguisé avec un objet du type message personnel comme "Sorry about yesterday", message commercial comme "Your account renewal now due" ou un message de non-distribution.



Pourquoi envoie-t-on un spam ?

Le spammeur envoie un spam parce que c'est rentable. Concrètement, il peut, en une seule campagne, envoyer des millions de courriels pour un coût négligeable (et s'il parvient à pirater les ordinateurs d'autres personnes pour envoyer le courriel, le coût est encore moindre). Même si un destinataire seulement sur les dix mille effectue un achat, cela s'avère rentable pour le spammeur.

Le spam est-il un réel problème ?

Le spam ne menace pas vos données de la même façon que les virus, mais il est nuisible à votre entreprise.

- Le spam représente une perte de temps pour le personnel. L'utilisateur sans protection anti-spam doit vérifier si tel courriel est un spam avant de le supprimer.
- L'utilisateur peut facilement ignorer ou même supprimer un courriel important, le confondant avec un spam.
- Le spam, comme le canular ou le virus de messagerie, utilise la bande passante et remplit inutilement les bases de données.
- Certains spams sont offensants pour l'utilisateur. Censé procurer un environnement de travail sain, l'employeur peut être tenu pour responsable.
- Le spammeur utilise souvent les ordinateurs d'autres personnes pour envoyer du spam ("piratage").



Piratage

Souvent, le spammeur pirate les ordinateurs d'autres utilisateurs et les utilisent pour envoyer du spam. A leur insu, les victimes du piratage bombardent ensuite de spam d'autres utilisateurs. Le spammeur fait en sorte de ne pas être suivi à la trace pour que ce soit l'entreprise possédant l'ordinateur piraté qui reçoive les plaintes et voie sa réputation ternie.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



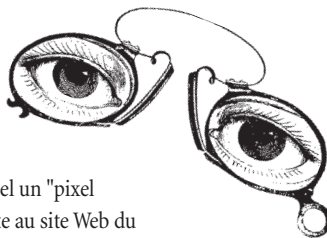
Références

Le spammeur sait ce que vous consultez

Afin de cibler sa campagne suivante, le spammeur veut savoir qui reçoit et qui ne reçoit pas ses messages.

Même si vous ne répondez pas au spam, le spammeur a des moyens de savoir si vous l'avez reçu.

- Si votre programme de messagerie est paramétré pour prévisualiser des messages (c'est-à-dire pour afficher le contenu du message dans une fenêtre située au-dessous de la liste des courriels), le spammeur peut voir que le courriel a été reçu.
- Si vous cliquez sur un lien qui sert à se désabonner d'une liste de diffusion, vous confirmez que votre adresse électronique est active. Le spammeur peut alors vendre votre adresse à d'autres.
- Le spammeur peut intégrer dans le courriel un "pixel invisible". Il s'agit d'un lien qui se connecte au site Web du spammeur dès que le courriel est lu ou prévisualisé.



Si vous ne voulez pas que le spammeur sache que ses courriels sont arrivés à destination, suivez les conseils de la section "Comment éviter le spam".

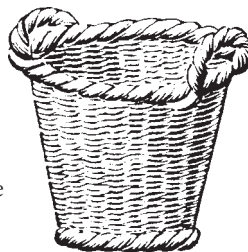
Logiciels anti-spam

Les programmes anti-spam parviennent à détecter les courriels non désirés et à les empêcher d'atteindre les boîtes de réception des utilisateurs.

Ces programmes utilisent une combinaison de méthodes servant à déterminer la probabilité pour qu'un courriel soit du spam. Ils parviennent à :

- Bloquer les courriels provenant d'adresses figurant sur liste noire. Il peut s'agir d'une liste disponible dans le commerce ou une liste "locale" d'adresses qui ont par le passé envoyé du spam dans votre entreprise.
- Vérifier si le courriel provient d'un nom de domaine ou d'une adresse Web authentique. Pour essayer d'éviter les programmes anti-spam, les spammeurs utilisent souvent de fausses adresses.
- Retrouver des mots-clés ou des groupes de mots qui reviennent dans le spam ("carte de crédit" ou "perdre du poids").
- Retrouver des motifs qui suggèrent que l'expéditeur du courriel essaie de déguiser ses mots (comme "hardc*re p0rn").
- Retrouver le code HTML inutile (le code utilisé pour l'écriture des pages Web) utilisé dans les courriels, les spammeurs l'utilisant souvent pour essayer de cacher leurs messages et semer la confusion dans les programmes anti-spam.

Ce type de programme combine toutes les informations qu'il trouve pour déterminer la probabilité qu'un courriel est du spam. Si cette probabilité est suffisamment élevée, il peut bloquer le courriel ou le supprimer en fonction des paramètres que vous avez choisis.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Un logiciel qui parvient à déterminer quels sont les courriels désirés

Certains logiciels anti-spam sont “adaptatifs”, c’est-à-dire qu’ils apprennent à différencier les objets que vous jugez acceptables de ceux non désirés.

Supposons qu’une entreprise pharmaceutique installe un logiciel anti-spam. Au début, le logiciel tente de détecter le spam en recherchant, par exemple, les mots suivants : *credit, free, consolidate, debt, mortgage, drugs, prescription, medication, doctor*. Il bloque les courriels contenant trop souvent ces mots-clés tout en permettant aux utilisateurs individuels de récupérer ceux qu’ils désirent lire.

Un employé du département recherche réalise qu’un courriel authentique relatif à un nouveau médicament a été bloqué et demande qu’il soit libéré. Le logiciel va dans ce cas mémoriser que cet utilisateur reçoit fréquemment des courriels sur des médicaments et, par conséquent, attribuer une pondération moindre aux termes relatifs aux médicaments lorsqu’il vérifiera le spam.

Dans le service financier, certains utilisateurs reçoivent des courriels contenant des termes financiers, ainsi le logiciel apprend alors à attribuer une pondération moindre à ces mots tout en continuant à bloquer pour ces utilisateurs les courriels relatifs aux médicaments.



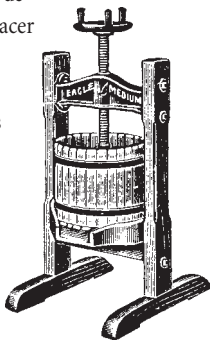
Les programmes anti-spam peuvent-ils bloquer des courriels authentiques ?

De nombreux utilisateurs s'inquiètent du fait que le logiciel anti-spam supprime des courriels personnels ou utiles. En réalité, votre courriel est en sécurité et vous pouvez même, si vous le souhaitez, voir le spam sélectionné.

Les programmes anti-spam peuvent être très précis. Ils peuvent généralement bloquer moins d'un courriel authentique sur dix mille, voire sur cent mille.

Même si le programme identifie de manière incorrecte un courriel comme du spam, il peut être configuré pour, au lieu de supprimer ce courriel, le placer dans une zone de "quarantaine".

L'administrateur peut alors décider de libérer ou de supprimer le courriel. Certains programmes permettent à chaque utilisateur de récupérer autant de courriels placés en quarantaine qu'ils le désirent.



Je veux ce spam !

Le spam de l'un peut être la lecture essentielle de l'autre.

Une personne travaillant pour une société financière peut souhaiter consulter les taux d'intérêt offerts par d'autres sociétés. Ou bien une société d'informatique peut souhaiter savoir si les spammeurs vendent des produits piratés.

Heureusement, vous pouvez personnaliser certains logiciels anti-spam pour qu'ils laissent passer le spam qui vous intéresse.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Les combines utilisées par les spammeurs

Les spammeurs cherchent en permanence des moyens pour déguiser leurs messages et tromper les logiciels anti-spam. Voici quelques-unes des techniques utilisées :

Perdu dans l'espace

Le spammeur place des espaces entre les lettres des mots qu'il souhaite cacher, par exemple "d r u g s", en espérant que le logiciel anti-spam ne lira pas les lettres en un mot. Cette combine est facile à détecter.



Le trou noir

Le spammeur utilise du code HTML (le code utilisé pour écrire les pages Web) pour insérer un espace entre les lettres, mais paramètre aussi la taille de l'espace sur zéro.

Ce que lit le programme anti-spam

```
V<font size=0>&nbsp;sp; </font>i<font size=0>
&nbsp;sp; </font>a<font size=0>&nbsp;sp: </font>g
<font size=0>&nbsp;sp; </font>r<font size=0>
&nbsp;sp; </font>a
```

Ce que vous voyez

Viagra

Les combines utilisées par les spammeurs

Encre invisible

Parfois, le spammeur veut que le lecteur consulte un message pendant que le programme anti-spam, lui, envoie un autre, plus innocent. Il utilise pour cela du code HTML pour insérer un message d'apparence innocent, mais dans la même couleur que l'arrière-plan.

Ce que lit le programme anti-spam

```
<body bgcolor=white> Viagra  
<font color=white>Hi, Johnny! It was really  
nice to have dinner with you. See you soon,  
love Mom</font></body>
```

Ce que vous voyez

Viagra



Le micropoint

Le spammeur insère une lettre supplémentaire au milieu du mot qu'il veut déguiser, mais utilise une très petite taille de caractères. Le programme anti-spam voit la lettre et lit le mot de façon incorrecte, mais le destinataire du courriel, lui, le lit très bien.

Retour à l'expéditeur

Le spammeur envoie volontairement son courriel à une adresse incorrecte, mais place votre adresse dans le champ "De". Le courriel ne peut pas être transmis, c'est pourquoi le fournisseur de services peut le renvoyer à ...vous.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Les combines utilisées par les spammeurs

Le jeu des numéros

Un spammeur peut écrire un mot en utilisant à la place de lettres ordinaires des codes HTML spéciaux. Par exemple, la lettre "a" peut être écrite en saisissant `a`.

Ce que que lit le programme anti-spam

```
&#86;<font size=0>&nbsp;</font>&#105;<font
size=0>&nbsp;</font>&#97;<font size=0>&nbsp;</font>&#103;<font size=0>&nbsp;</font>
&#114;<font size=0>&nbsp;</font>&#97
```

Ce que vous voyez

Viagra

Découpage du texte

Le spammeur utilise des tableaux HTML pour découper le texte en fines colonnes verticales, comme si le message avait été passé au travers d'une déchiqueteuse.

Ce que que lit le programme anti-spam

V	i	a	g	r	a	
S	a	m	p	l	e	
F	r	e	e		s	

Ce que vous voyez

Viagra
samples
free

Association du spam et des virus

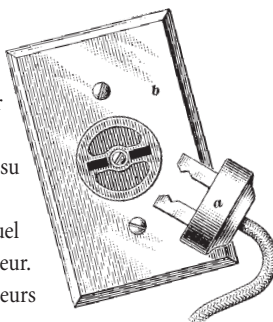
Il arrive que les spammeurs et les auteurs de virus collaborent pour créer encore plus de dégâts dans les messageries.

Les virus peuvent constituer de nouvelles opportunités pour le spam. Un auteur de virus peut, par exemple, écrire un virus qui permette à d'autres utilisateurs de prendre le contrôle d'un ordinateur à l'insu de l'utilisateur légitime. Si ce virus réussit à infecter un ordinateur, il envoie un message à l'auteur de virus, lequel peut envoyer sa liste d'ordinateurs infectés à un spammeur. Les spammeurs n'ont plus alors qu'à utiliser ces ordinateurs pour envoyer du spam.

Plus de 30 % du spam est maintenant envoyé par l'intermédiaire d'ordinateurs compromis comme ceux-là. De cette manière, les spammeurs deviennent plus difficiles à suivre à la trace.

Les techniques des spammeurs peuvent également servir aux créateurs de virus. Un auteur de virus peut ainsi envoyer un virus par courriel à un grand nombre d'utilisateurs en se servant de la liste d'adresses d'un spammeur. Avec autant de destinataires, il est fort probable qu'un grand nombre d'entre eux activeront le virus, garantissant ainsi un réacheminement et une propagation rapides.

Il semble qu'on ait des preuves de collusion entre les spammeurs et les auteurs de virus. Le virus *Mimail-L*, par exemple, a tenté de lancer une attaque par déni de service sur plusieurs sites Web anti-spam.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Comment éviter le spam

Utilisez un logiciel anti-spam

Le logiciel anti-spam peut réduire le nombre de courriels non désirés, surtout s'il utilise vos commentaires pour "apprendre" à différencier les courriels authentiques du spam.

N'effectuez jamais d'achats à partir d'un spam

En effectuant un achat, vous aidez au financement du spam. Votre adresse électronique peut aussi être ajoutée dans des listes vendues à d'autres spammeurs pour que vous receviez encore plus de courriers-poubelles. Pire encore, vous pouvez être victime d'une fraude.



En cas d'expéditeur inconnu, supprimez le courriel

Non seulement la plupart des spams sont une gêne, mais ils peuvent aussi parfois contenir un virus qui endommage l'ordinateur lorsque le courriel est ouvert.

Ne répondez jamais à un spam ou ne cliquez jamais sur les liens

Si vous répondez à un spam, même pour vous désabonner de la liste de diffusion, vous confirmez que votre adresse électronique est valide, ce qui encourage davantage encore l'envoi de spam.

Choisissez de ne pas recevoir d'autres informations ou offres

Lorsque vous remplissez un formulaire sur n'importe quel site Web, recherchez toujours la case à cocher qui permet de choisir d'accepter ou non d'autres informations ou offres. Cochez ou décochez cette case selon les besoins.

Comment éviter le spam

N'utilisez jamais la prévisualisation de la visionneuse de courriels

La plupart des spammeurs parviennent à suivre à la trace la visualisation d'un message, même si vous ne cliquez pas sur le courriel. L'option de prévisualisation ouvre effectivement le courriel et permet au spammeur de savoir que vous recevez ses messages. Lorsque vous vérifiez votre courriel, essayez de déterminer d'après l'objet seulement s'il s'agit ou non d'un spam.

Utilisez le champ "cc" ("bcc" en anglais) lorsque vous envoyez un courriel à plusieurs personnes à la fois

Le champ "cc" ou copie conforme invisible masque la liste de destinataires pour les autres utilisateurs. Si vous placez les adresses dans le champ "À", le spammeur peut les recueillir et les ajouter aux listes de diffusion.

Ne donnez jamais votre adresse électronique sur Internet

Ne mentionnez jamais votre adresse électronique sur les sites Web, listes de newsgroups ou autres forums publics en ligne car le spammeur utilise des programmes qui surfent sur Internet pour y trouver des adresses.

Ne donnez votre adresse principale qu'aux personnes de confiance

Ne confiez votre adresse électronique principale qu'à vos amis et collègues.

Utilisez une ou deux adresses électroniques "secondaires"

Si vous remplissez des formulaires d'inscription sur Internet ou participez à des enquêtes sur des sites dont vous ne souhaitez pas recevoir d'autres informations, utilisez une adresse électronique secondaire. Cette précaution protège votre adresse principale du spam.



Virus



Spam



Canulars



Sécurité



Références

Canulars et escroqueries

Si vous recevez un courriel qui vous prévient d'un nouveau virus aux consonances improbables, vous offre un téléphone portable gratuit ou vous demande de mettre à jour les détails de votre compte en banque, c'est que vous êtes la victime d'un canular. Le courriel-canular peut interrompre votre activité, surcharger les systèmes de messagerie ou encore vous amener par la ruse à donner à des criminels vos codes d'accès et vos mots de passe.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Les canulars de virus

Les canulars de virus signalent des virus qui n'existent pas. Le canular type est un courriel qui :

- Vous avertit de l'existence d'un nouveau virus indétectable et extrêmement destructeur.
- Vous suggère d'éviter la lecture des courriels avec des objets comme Join the Crew ou Budweiser Frogs.
- Prétend que tel avertissement a été émis par une grande société informatique, un fournisseur d'accès Internet ou un organisme d'Etat comme IBM, Microsoft, AOL ou la FCC (équivalent américain de l'ART, qui régule les télécoms).
- Prétend qu'un nouveau virus peut réaliser une action improbable. Par exemple, *A moment of silence* annonce "qu'aucun programme n'a besoin d'être échangé pour qu'un autre ordinateur soit infecté".
- Emploie un jargon informatique pour décrire les effets d'un virus : par exemple, *Good Times* annonce que le virus peut faire rentrer le processeur de votre PC dans une "boucle binaire infinie de complexité".
- Vous conseille vivement de faire suivre l'avertissement aux autres utilisateurs.



Canular ou pas ?

Un courriel intitulé *Rush-Killer virus alert* a commencé à circuler le 1er avril 2000. Il prévenait de l'existence d'un virus qui pouvait prendre le contrôle de votre modem et composer le 911 (numéro des urgences aux Etats-Unis) et conseillait vivement de faire suivre l'alerte. Le courriel présentait tous les signes extérieurs d'un canular. Et pourtant, ce virus était réel. Distinguer un canular d'un vrai virus n'est pas chose facile ; il est donc recommandé de suivre les conseils donnés à la fin de ce chapitre, dans la section "Comment éviter les canulars".

Ne jamais négliger l'importance d'un canular

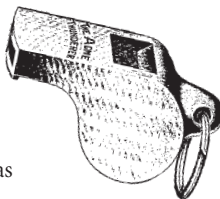
Le canular peut être aussi problématique et coûteux qu'un virus authentique.

Si un utilisateur fait suivre un avertissement-canular à ses amis et collègues, il peut s'en suivre un déluge de courriels qui va submerger les serveurs et les faire tomber en panne. L'effet est donc semblable à celui du vrai virus *Sobig*, à la seule différence que l'auteur du canular n'a pas eu besoin de programmer le moindre code.

L'utilisateur final n'est pas le seul à réagir de façon excessive. Les entreprises qui reçoivent fréquemment des canulars prennent parfois des mesures drastiques comme la fermeture de leur serveur de messagerie ou de leur réseau, ce qui a pour effet de paralyser les transmissions plus efficacement que n'importe quel authentique virus, empêchant par là-même l'accès à des courriels potentiellement importants.

De faux avertissements peuvent aussi disperser les efforts dans la lutte contre les vraies menaces virales.

Par ailleurs, les canulars peuvent s'avérer remarquablement persévérants. Et les canulars n'étant pas des virus, votre logiciel ne peut ni les détecter ni les désactiver.



Les canular inspirent-ils des virus ?

Un canular peut inspirer une réelle menace virale et vice-versa. Lorsque le canular *Good Times* a fait les gros titres, certains programmeurs de virus ont attendu que cette rumeur soit entièrement étouffée pour écrire un vrai virus du même nom (certains éditeurs antivirus l'ont appelé *GT-Spoof*).



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Piratage de pages

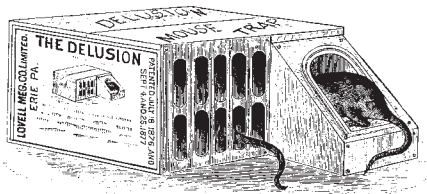
Le piratage de pages consiste à répliquer des pages Web de renom pour captiver l'attention de l'utilisateur et le rediriger vers d'autres sites Web.

Le pirateur de pages copie des pages d'un site Web de renom et les place sur un nouveau site qui semble légitime. Il enregistre ensuite ce nouveau site auprès des principaux moteurs de recherche afin que l'utilisateur effectuant une recherche le retrouve et suive les liens présents. Lorsque l'utilisateur arrive sur le site Web, il est automatiquement redirigé vers un site différent contenant de la publicité ou des offres de différents services.

Généralement, le piratage de pages agace l'utilisateur et le met face à du contenu offensant. Il réduit par ailleurs les recettes des sites Web légitimes et l'utilité des moteurs de recherche.

Dans certains cas, le piratage de pages peut être utilisé pour le "*phishing*" (voir page suivante).

Sachez que si vous utilisez un signet ou un "favori", ou si vous entrez directement l'adresse du site Web (son URL), vous ne tomberez pas dans le piège du piratage de pages.



Souricière

Supposons que vous soyez redirigé vers un faux site Web et que les boutons de retour ou de fermeture ne vous permettent plus d'en sortir. Vous êtes victime du coup de la souricière.

Pour quitter cette page, saisissez une adresse dans le champ "Adresse", utilisez un signet ou ouvrez la liste des adresses récemment visitées et sélectionnez celle qui figure juste après la dernière visitée. Pour récupérer l'utilisation des boutons de retour ou de fermeture, fermez le navigateur ou redémarrez l'ordinateur.

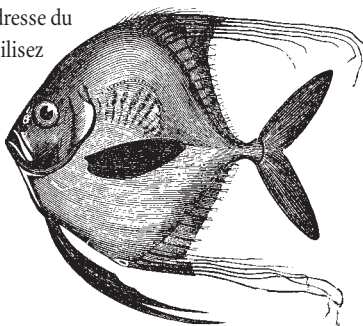
Phishing

Le phishing consiste à employer des faux courriels et sites Web pour vous inciter à fournir des informations confidentielles ou personnelles.

En général, vous recevez un courriel semblant provenir d'une organisation reconnue, telle une banque. Le courriel contient ce qui semble être un lien vers le site Web de l'organisation. En revanche, si vous suivez le lien, vous vous retrouvez connecté à une réplique du site Web. Tous les détails que vous saisissez alors, tels que les numéros de comptes, les numéros d'identification personnels ou les mots de passe peuvent être volés et utilisés par les pirates qui ont créé ce faux site.

Il faut toujours se méfier des liens envoyés dans des courriels. Au lieu de cliquer sur un lien, saisissez l'adresse du site Web dans le champ "Adresse" ou utilisez un signet ou un lien "favoris", et vous serez sûr de vous connecter au véritable site.

Un logiciel anti-spam peut aussi aider à bloquer les courriels de phishing.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



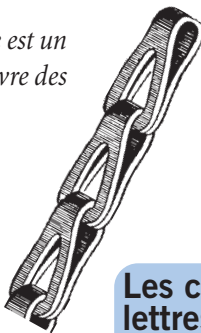
Références

Chaîne de lettres

Une chaîne de lettres électronique est un courriel qui vous incite à faire suivre des copies à d'autres personnes.

Voici les principaux types de chaînes de lettres :

- **Canulars.** Les chaînes de lettres peuvent avertir d'attaques terroristes, d'escroqueries impliquant des numéros de téléphone surtaxés ou de vols depuis des guichets automatiques. Toutes sont soit des canulars délibérés soit des légendes urbaines.
- **Faux cadeaux gratuits.** Certaines lettres prétendent à tort que des sociétés offrent des voyages, des téléphones portables gratuits ou bien des récompenses si vous faites suivre des courriels.
- **Pétitions.** Il s'agit généralement de pétitions contre les lois proposées. Même si elles sont authentiques, elles continuent de circuler longtemps après leur date d'expiration.
- **Blagues et farces.** La lettre "Internet cleaning" prétendait qu'Internet serait hors d'usage le 1er avril pour cause de maintenance.



Les chaînes de lettres sont-elles réellement problématiques ?

Les chaînes de lettres ne menacent pas votre sécurité, mais elles peuvent :

- Vous faire perdre du temps ou détourner votre attention des courriels authentiques.
- Créer inutilement du trafic de courriels et ralentir vos serveurs de messagerie.
- Diffuser de fausses informations.
- Encourager l'envoi de courriels à certaines adresses de façon à ce que ces dernières soient inondées de courriels non sollicités.

Comment éviter les canulars

Adoptez une stratégie de sécurité concernant les alertes virales

Mettez en place dans l'entreprise une stratégie de sécurité à propos des alertes virales, par exemple :

“Faites suivre les alertes virales, quel qu'en soit le type, uniquement au *responsable sécurité*. Peu importe si cette alerte provient d'un distributeur antivirus ou si elle a été validée par une société d'informatique importante ou par votre meilleur ami. TOUTES les alertes virales doivent être transmises seulement au *nom de la personne responsable* qui doit ensuite avertir tout le monde. Une alerte virale provenant de toute autre source doit être ignorée.”

Renseignez-vous régulièrement sur les canulars

Renseignez-vous sur les canulars en visitant sur notre site Web les pages qui leur sont consacrées : www.sophos.fr/virusinfo/hoaxes

Ne faites jamais suivre une chaîne de lettres

Ne faites jamais suivre une chaîne de lettres, même si des récompenses sont offertes ou si on y prétend diffuser des informations utiles.

Ne faites confiance à aucun lien de courriel non sollicité

Si vous désirez visiter le site Web de votre banque ou tout site sur lequel vous saisissez des mots de passe ou des informations confidentielles, ne cliquez jamais sur les liens présents dans les courriels non sollicités ou les forums. Saisissez vous-même votre adresse ou utilisez un signet ou un lien “favoris”.



Virus



Spam



Canulars

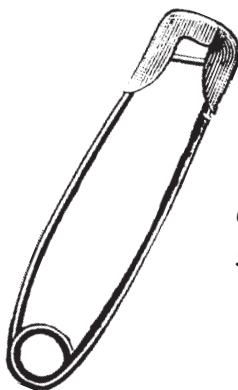


Sécurité



Références

Astuces pour une informatique sécurisée



Mise à part l'utilisation d'un logiciel antivirus, il existe de nombreuses mesures simples pour se protéger soi-même et son entreprise contre les virus et les vers. Voici nos principaux conseils pour une informatique sans souci.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Astuces pour une informatique sécurisée

Ne lancez jamais de programmes ou de documents non sollicités

Quand vous ne savez pas si une entité contient ou non un virus, supposez qu'elle en contient un. Ordonnez à vos employés de ne pas télécharger depuis Internet des programmes ou des documents non autorisés, des économiseurs d'écrans ou des blagues. Adoptez une politique qui dicte que tous les programmes doivent être autorisés par un responsable informatique et vérifiés avant leur utilisation.

N'utilisez jamais de documents au format .doc et .xls

Enregistrez les documents Word au format RTF et les feuilles Excel au format CSV car ces formats ne prennent pas en charge les macros et ne peuvent donc pas diffuser de virus de document. Dites à vos correspondants de vous envoyer des fichiers RTF et CSV. Mais prenez garde ! Certains virus de document déguisent le format. Pour travailler en toute sécurité, utilisez des fichiers texte seulement.

Utilisez des correctifs logiciels pour colmater les failles de sécurité

Soyez à l'affût des actualités sur la sécurité et téléchargez les correctifs. De tels correctifs comblent souvent les trous de sécurité qui peuvent vous rendre vulnérables aux virus et aux vers Internet. Il est conseillé à tout directeur informatique de s'abonner aux listes de diffusion des éditeurs de logiciels comme celle présente sur www.microsoft.com/technet/security/bulletin/notify.asp. Les utilisateurs à domicile possédant des ordinateurs Windows peuvent visiter windowsupdate.microsoft.com, où vous pouvez effectuer un contrôle de votre PC pour y rechercher les failles de sécurité et savoir quels correctifs installer.

Astuces pour une informatique sécurisée

Bloquez à la passerelle les fichiers avec extensions doubles

Certains virus déguisent le fait qu'ils sont des programmes en utilisant après leurs noms de fichiers une extension double, comme .TXT.VBS. Par exemple, un fichier comme LOVE-LETTER-FOR-YOU.TXT.VBS ressemblait, à première vue, à un fichier texte ou à un graphique inoffensif. Bloquez à la passerelle de messagerie tout fichier portant une double extension.

Bloquez à la passerelle de messagerie les fichiers non désirés

De nombreux virus utilisent maintenant les extensions VBS (Visual Basic Script) et SHS (Windows Scrap Object) pour se propager. Il y a de fortes chances pour que votre entreprise n'ait pas besoin de recevoir de l'extérieur ces types de fichiers, vous pouvez donc les bloquer à la passerelle de messagerie.

Abonnez-vous à un service d'alerte par courriel

Un service d'alerte peut vous avertir des nouveaux virus et vous proposer des identités virales qui permettront à votre logiciel antivirus de les détecter. Sophos dispose d'un service d'alerte gratuit. Pour plus de détails, reportez-vous à www.sophos.fr/virusinfo/notifications

Ayez un réseau distinct pour les machines Internet

Gérez des réseaux distincts pour les ordinateurs reliés à Internet et pour ceux qui ne le sont pas. Ainsi, vous réduisez le risque que l'utilisateur ne télécharge des fichiers infectés et diffuse des virus sur votre réseau principal.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Astuces pour une informatique sécurisée

Utilisez des pare-feu et/ou des routeurs

Un pare-feu n'admet dans votre entreprise que le trafic autorisé. Un routeur contrôle le flux de paquets d'informations provenant d'Internet.

Configurez votre navigateur Internet pour la sécurité

Désactivez les applets Java ou ActiveX, les cookies, etc., ou demandez à être averti si du code comme celui-ci est en cours de fonctionnement. Par exemple, dans Microsoft Internet Explorer, sélectionnez **Outils|Options Internet|Sécurité|Niveau personnalisé** et sélectionnez les paramètres de sécurité désirés.

Effectuez des sauvegardes de tous les programmes et données

Si vous êtes infecté par un virus, vous pourrez ainsi récupérer tous les programmes et toutes les données perdues.

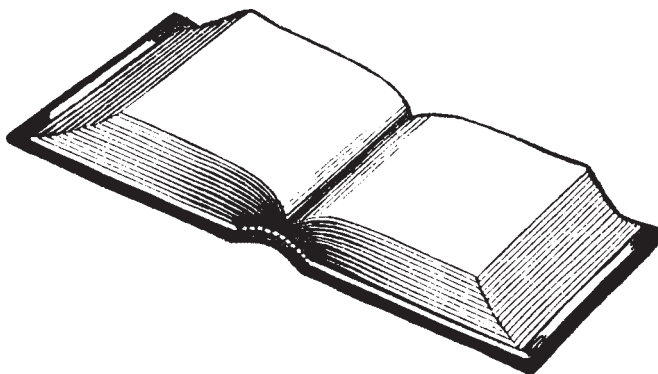
Changez la séquence de démarrage de votre ordinateur

La plupart des ordinateurs tentent tout d'abord de se lancer depuis le lecteur de disquette (le lecteur A:). Demandez au responsable informatique de changer les paramètres de votre ordinateur pour qu'il s'initialise tout d'abord depuis le disque dur. Ensuite, si une disquette infectée reste dans l'ordinateur, ce dernier ne pourra être infecté par aucun virus de secteur de démarrage.

Protégez toujours une disquette en écriture avant de la transmettre

Une disquette protégée en écriture ne peut pas être infectée.

Glossaire



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

ActiveX

Technologie Microsoft qui accroît les capacités de votre navigateur Web.

Amorçage

Processus de chargement du système d'exploitation depuis le disque lors de la mise sous tension de l'ordinateur.

Applet

Petite application. On parle habituellement d'applets Java (voir ce nom).

Applet Java

Petite application généralement utilisée pour créer des effets sur les pages Web. Les applets sont exécutés par le navigateur dans un environnement sûr (voir Sandbox) et ne peuvent apporter de changements sur votre système.

Application Java

Programme Java qui peut exécuter les fonctions complètes qu'on attend de lui, comme la sauvegarde de fichiers sur un disque.

ASCII

American Standard Code for Information Interchange. Système normatif de représentation de lettres et de symboles.

Attaque dictionnaire

Programme qui bombarde un serveur de messagerie avec des adresses électroniques générées par ordre alphabétique dans l'espoir de deviner correctement certaines d'entre elles. La même méthode peut servir à deviner des mots de passe.

Attaque par déni de service

Tentative pour empêcher l'utilisation d'un système de messagerie ou d'un serveur Web en envoyant des messages ou des pièces jointes inhabituels ou excessifs.

BIOS

Basic Input/Output System (système de base d'entrées/sorties). Niveau inférieur du logiciel directement interfacé avec le matériel.

Canular

Communication, souvent par courriel, intentionnellement trompeuse.

CGI	Common Gateway Interface. Mécanisme permettant au serveur Web d'exécuter des programmes ou des scripts et d'en envoyer le résultat à un navigateur Web.
Cheval de Troie	Programme informatique ayant des effets (indésirables) non décrits dans ses spécifications.
Cheval de Troie de porte dérobée	Programme de cheval de Troie (voir ce nom) qui donne à l'utilisateur distant un accès non autorisé à un ordinateur et qui lui permet de le contrôler.
Collecte	Contrôle d'Internet à la recherche d'adresses électroniques pouvant être placées sur les listes de diffusion des spammeurs.
Contrôle complexe du vocabulaire	Fonction du logiciel anti-spam qui retrouve les mots souvent utilisés dans le spam, même si des lettres ont été remplacées par des nombres ou des caractères semblables (comme "Interest r@te").
Contrôle HTTP	Contrôle en temps réel du trafic HTTP pour s'assurer que les pages Web que vous visualisez ou téléchargez ne contiennent pas de virus.
Cookie	Petit ensemble de données qui renferme des informations sur l'ordinateur de l'utilisateur. Les cookies sont généralement utilisés pour permettre à un site Web de suivre à la trace les visites et les caractéristiques des utilisateurs.
CSV	Comma Separated Values. Format de fichier dans lequel les valeurs (par exemple, celles d'une feuille de calcul Excel) apparaissent séparées par des virgules. Ce format ne supporte pas les macros et ne peut donc pas propager de virus de macro.
Disque dur	Disque magnétique scellé généralement placé à l'intérieur d'un ordinateur et servant à stocker des données.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Disquette

Disque magnétique amovible souple utilisé pour stocker des données.

Enregistrement d'amorçage maître

Aussi appelé secteur de partition. Il s'agit du premier secteur physique du disque dur à être chargé et exécuté lorsqu'un PC est initialisé et aussi de la partie essentielle du code de démarrage.

Faux positif

Rapport signalant qu'un virus a été trouvé (ou qu'un courriel est du spam) alors que ce n'est pas le cas.

Filtrage bayésien

Approche statistique consistant à déterminer si un courriel est un spam (fondée sur la théorie de la probabilité bayésienne).

FTP

File Transfer Protocol. Système permettant aux utilisateurs d'Internet de se connecter à des sites distants pour télécharger des fichiers (d'un serveur Web au terminal ou dans le sens inverse).

Hacker

Pirate. Personne qui tente délibérément de violer la sécurité informatique, généralement pour provoquer des perturbations ou récupérer des informations confidentielles comme des détails financiers. Au départ, le mot "hacker" faisait référence à toute personne passionnée par la technologie informatique. Aujourd'hui, ce terme est fréquemment utilisé par le public et les journalistes pour désigner des personnes mal intentionnées.

Ham

Courriel qu'un destinataire ne considère pas comme du spam (voir ce nom).

HTML

Hypertext Markup Language. Format de la plupart des documents sur le Web.

HTTP

Hypertext Transport Protocol. Protocole utilisé par les serveurs Web pour rendre les documents d'un site disponibles pour les navigateurs.

Identité virale	Description des caractéristiques d'un virus utilisée pour sa reconnaissance.
Internet	Réseau composé de nombreux réseaux reliés entre eux. <i>Internet</i> est de loin le plus vaste de ces réseaux.
Java	Langage de programmation indépendant des plates-formes développé pour le Web par Sun Microsystems. Les programmes écrits en Java sont soit des applications soit des applets (petites applications).
Liste blanche	Liste d'adresses électroniques externes, d'adresses IP et de domaines à partir desquels les courriels sont acceptés sans faire l'objet d'aucune vérification de spam et/ou de virus.
Liste grise	Les expéditeurs de courriels non placés en liste noire (exclus) ou en liste blanche (acceptés) peuvent être placés dans une liste grise et être sommés de prouver qu'ils envoient des courriels légitimes.
Liste noire	Liste d'adresses électroniques et de domaines desquels aucun courriel n'est accepté.
Liste "trou noir"	Liste publiée, généralement commerciale, d'adresses connues pour être des sources de spam. Voir aussi Liste "trou noir" en temps réel.
Liste "trou noir" en temps réel	Real-time blackhole list (RBL). Liste rejetant tout courriel, valide ou non, provenant d'adresses connues pour envoyer du spam ou accueillir des spammeurs. Ceci peut inciter les fournisseurs de service Internet à prendre des mesures anti-spam.
Macro	Séries d'instructions au sein de fichiers de données qui peuvent réaliser automatiquement des commandes de programme, par exemple, l'ouverture ou la fermeture de fichiers.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Mail drop

Adresse électronique conçue pour recevoir des réponses à du spam. Afin d'éviter la détection, le spammeur annule ensuite le compte à partir duquel le spam a été envoyé.

Modem

MODulateur/DEModulateur qui convertit les données informatiques dans une forme adaptée à la transmission par ligne téléphonique, liaison radio ou satellite.

Mot de passe

Suite de caractères donnant accès à un système.

Munging

Déguisement d'adresses électroniques afin qu'elles ne puissent pas être collectées. On indique aux destinataires comment décoder l'adresse.

Navigateur Web

Programme utilisé pour accéder aux informations sur le Web, il s'agit donc de la partie client du Web.

Newsgroup

Forum électronique où les participants publient des articles et des suivis d'articles sur des sujets donnés.

Obfuscation

Tentative du spammeur pour cacher les messages de manière à ce qu'ils ne soient pas détectés. Parfois utilisé pour désigner le déguisement des adresses électroniques pour que le spammeur puisse les collecter.

Open-relay

Relais non protégé. Serveur de messagerie SMTP permettant le relais de messages électroniques à un tiers. Les spammeurs peuvent pirater ces serveurs et les utiliser pour envoyer du spam.

Ordinateur palmtop

Ordinateur suffisamment petit pour tenir dans la paume (palm) de la main.

Ordinateur portable

Ordinateur portable suffisamment petit pour être utilisé sur les genoux.

Pare-feu

Système de sécurité placé entre Internet et le réseau d'une entreprise, ou au sein même d'un réseau, pour ne laisser passer que le trafic réseau autorisé.

Passerelle	Ordinateur servant au transfert de données (par exemple, d'une passerelle de messagerie, par laquelle transitent tous les courriels parvenant à une entreprise) ; il peut aussi s'agir d'un ordinateur qui convertit des données d'un protocole dans un autre.
PC	Pour Personal Computer ou ordinateur personnel. Ordinateur de bureau ou portable pour une utilisation individuelle.
PDA	Personal Digital Assistant. Petit appareil informatique mobile qui s'utilise la plupart du temps pour gérer les données des carnets d'adresses ou des calendriers.
Phishing	Combine consistant à amener l'utilisateur par la ruse à soumettre des informations confidentielles ou des mots de passe en créant une réplique d'un site Web légitime.
Pièce jointe	Fichier document, feuille de calcul, graphique, programme joint au message d'un courriel.
Pixel invisible	Petit graphique inséré dans un courriel ou sur une page Web alertant le spammeur lorsqu'un message est lu ou prévisualisé.
Portable notebook	Ordinateur encore plus petit qu'un ordinateur portable.
Porte dérobée	Moyen non documenté de contourner le système de contrôle d'accès habituel d'un ordinateur. Voir cheval de Troie de porte dérobée.
Pot de miel	Système informatique placé sur Internet pour attirer et piéger les spammeurs et les pirates.
Programme	Série d'instructions qui indique à un ordinateur les actions à réaliser.
RAM	Random Access Memory. Forme de mémoire temporaire d'un ordinateur. Cette mémoire vive agit comme l'espace de travail de la machine mais, une fois l'ordinateur éteint, les données qui y sont stockées sont perdues.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

ROM

Read Only Memory. Forme de mémoire permanente de l'ordinateur. Cette mémoire morte s'utilise généralement pour stocker le logiciel de démarrage d'un ordinateur.

RTF

Rich Text Format. Format de fichier document qui ne supporte pas les macros et ne peut donc pas propager de virus de macros.

Sandbox

Mécanisme servant à exécuter des programmes en environnement contrôlé, en particulier au moyen d'applets Java.

Sauvegarde

Copie des données d'un ordinateur utilisée pour recréer des données perdues, égarées, altérées ou effacées.

Scanner de virus

Programme détectant les virus. La plupart des scanners sont spécifiques aux virus, c'est-à-dire qu'ils identifient les virus qu'ils connaissent déjà. Voir aussi Scanner heuristique.

Scanner heuristique

Programme qui détecte les virus en utilisant des règles générales sur ce que sont les virus ou sur leur comportement.

Secteur de démarrage

Partie du système d'exploitation qui est lue en premier par le disque lorsqu'un ordinateur est mis sous tension. Le programme stocké dans le secteur de démarrage est ensuite exécuté, ce qui entraîne le chargement du reste du système d'exploitation.

Secteur de démarrage DOS

Secteur de démarrage qui charge le système d'exploitation DOS dans la mémoire RAM du PC. Il s'agit d'un point d'attaque courant des virus de secteur de démarrage.

Serveur de fichiers

Ordinateur fournissant un stockage centralisé de données et, souvent, d'autres services aux postes de travail d'un réseau.

Serveur proxy	Serveur qui envoie des requêtes à Internet au nom d'une autre machine. Il se situe entre l'entreprise et Internet et peut être utilisé pour des raisons de sécurité.
Serveur Web	Ordinateur connecté à Internet qui met à disposition les documents du Web, au moyen généralement du réseau HTTP.
SHS	Extension des fichiers "scrap object" de Windows. Les fichiers SHS peuvent renfermer du code de quasiment tout type et s'exécutent automatiquement si vous cliquez dessus. L'extension peut être cachée.
Signature numérique	Moyen de s'assurer qu'un message n'a pas fait l'objet de manipulations et qu'il provient bien de l'expéditeur indiqué.
SMTP	Simple Mail Transport Protocol. Système de distribution des courriels Internet.
Somme des contrôles	Valeur calculée à partir d'un ou de plusieurs élément(s) de données pouvant être utilisée pour vérifier que ces données n'ont pas été altérées.
Spam	Courrier commercial non sollicité (UCE pour Unsolicited Commercial Email) et courrier de masse non sollicité (UBE pour Unsolicited Bulk Email).
Spambot	Programme que les spammeurs utilisent pour collecter des adresses électroniques sur Internet.
Spoofing	Littéralement usurpation. Falsification dans un courriel de l'adresse de l'expéditeur. L'usurpation peut servir à cacher l'origine du spam ou à convaincre les destinataires qu'un courriel nuisible provient d'une source fiable.
Spyware	Logiciel espion qui suit à la trace l'activité de l'utilisateur et rapporte les informations à d'autres entités comme des annonceurs. Le suivi est généralement caché de l'utilisateur du logiciel.



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

Station de travail

Ordinateur pour utilisateur autonome souvent relié à un réseau.

Système d'exploitation Programme qui contrôle l'utilisation des ressources matérielles de l'ordinateur et effectue des fonctions de base telles que la maintenance des listes de fichiers et l'exécution des programmes.

Tarpit Serveur de messagerie délibérément lent dont le but est de prendre au piège les spammeurs qui collectent des programmes.

Tarpitting Surveillance du trafic de la messagerie pour identifier les adresses suspectées d'envoyer un gros volume de courriels pouvant être du spam.

TCP/IP Transmission Control Protocol/Internet Protocol. Nom collectif pour les protocoles Internet standard.

Téléchargement Transfert de données d'un ordinateur (serveur) vers un autre ordinateur (terminal).

URL Uniform Resource Locator. Adresse d'un site Web.

VBS Visual Basic Script. Code incorporé à une application, un document ou une page Web pouvant s'exécuter dès que la page est visualisée.

Ver Programme qui se diffuse en multiples exemplaires. A la différence du virus, le ver ne requiert pas de programme hôte.

Vérification DNS inversée Vérification de l'adresse de l'expéditeur du courriel dans une base de données de systèmes de noms de domaines pour s'assurer qu'elle provient d'un nom de domaine ou d'une adresse Web valide.

Virus Programme qui a la capacité de se répandre sur les ordinateurs et sur les réseaux en se greffant sur un autre programme et en créant ses propres répliques.

Virus compagnon	Virus exploitant le fait que lorsque deux fichiers programme portent le même nom, le système d'exploitation utilise leur extension pour décider lequel exécuter. Par exemple, les ordinateurs sous DOS exécutent de préférence un fichier .com plutôt qu'un fichier .exe. Le virus crée donc un fichier .com qui contient le code viral et lui donne le même nom que le .exe existant.
Virus de programme	Virus informatique qui se greffe sur un autre programme informatique et qui s'active lorsque ce programme est exécuté.
Virus de redirection	Virus qui bouleverse les entrées d'un répertoire de façon à ce qu'elles pointent vers le code du virus, permettant à celui-ci de s'exécuter.
Virus de secteur de démarrage	Type de virus dérégulant le processus d'amorçage.
Virus furtif	Virus dissimulant sa présence à l'utilisateur de l'ordinateur et aux programmes antivirus, en dérivant généralement les services d'interruption.
Virus macro	Virus employant les macros d'un fichier de données pour s'activer et se greffer sur d'autres fichiers de données.
Virus multimode	Virus qui infecte à la fois les secteurs et les fichiers programme.
Virus parasite	Voir Virus de programme.
Virus polymorphe	Virus qui se modifie lui-même. En changeant son propre code, le virus essaie de se rendre plus difficile à détecter.
Virus résident en mémoire	Virus restant en mémoire après s'être activé et après la fermeture de son programme hôte (à la différence des autres virus qui sont activés seulement lorsqu'une application infectée est exécutée).



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

WAP

Wireless Application Protocol. Protocole de type Internet qui fournit des informations aux téléphones mobiles et aux organisateurs.

Web

Voir World wide web.

World wide web

Système hypertexte distribué utilisé pour la lecture de documents sur Internet.

WWW

Voir World wide web.

Zombie

Ordinateur peu sûr piraté et utilisé pour envoyer du spam ou lancer une attaque par déni de service (voir ce nom).

Index

C

- canular de virus 42
 - effets secondaires 43
- canulars 41
 - canulars de virus 42, 43
 - chaîne de lettres 46
 - éviter 47
 - phishing 45
 - piratage de pages 44
- chaîne de lettres 46
- cheval de Troie 7
 - de porte dérobée 15
- cookies 16

D

- déni de service 8

F

- filtre anti-spam 31
 - adaptatif 32

H

- HTML
 - et le spam 34, 36

J

- Jini 18

L

- logiciel adaptatif 32
- logiciel anti-spam 31
 - adaptatif 32
- logiciel antivirus 20
 - heuristique 20
- logiciel heuristique 20

O

- ordinateur portable 19

P

- phishing 45
- pièces jointes aux courriels 12
- piratage de pages 44
- pixel invisible 30
- PocketPC 19

R

- règles de sécurité 49–52



Virus



Spam



Canulars



Sécurité



Références



Virus



Spam



Canulars



Sécurité



Références

S

sites web

faux 44, 45

piratage de pages 44

souricière 44

spam

combines de déguisement 34–36

défini 28

effets secondaires 29

et virus 37

éviter 38–39

spyware 16

T

téléphones mobiles 17

V

ver 7

internet 14

ver Internet 14

virus

dans des pièces jointes 12

dans un programme 11

de démonstration 24

de document 11

de messagerie 12, 13

de programme 11

de secteur de démarrage 11

de téléphone mobile 17

défini 6

diffusé par messagerie 12, 13

effets secondaires 8–9

et spam 37

historique 22

"inoffensif" 24

prévention 20, 25, 49–52

secteur de démarrage 11

sur ordinateur portable 19

virus macro, voir virus de document