La sécurité du poste de travail informatique

Spécificités de la communication électronique

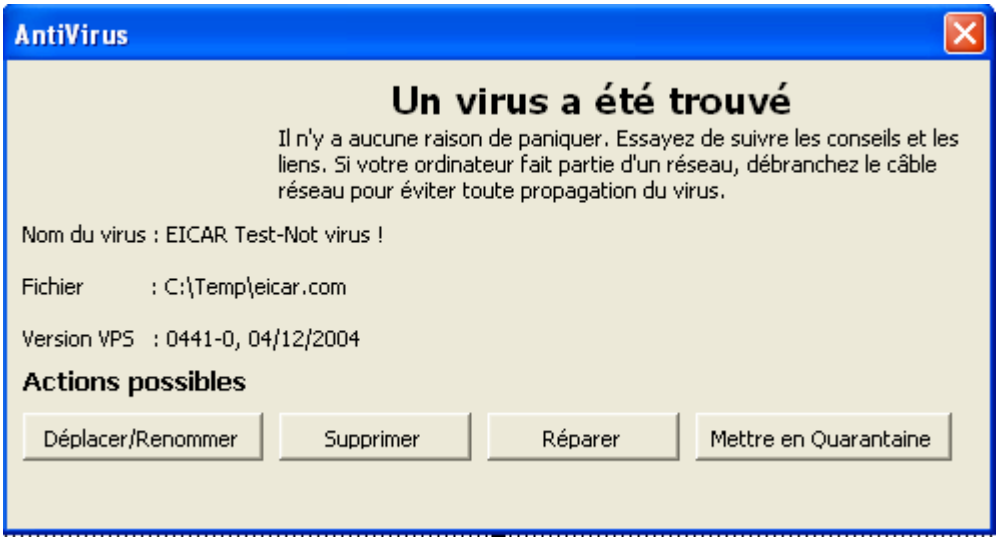
Propriétés	Description
Intitulé long	Prévention et comportement à adopter face aux dangers informatiques liés à la communication entre des ordinateurs.
Formation concernée	Classes de première Sciences et technologies de la gestion (STG)
Matière	Information et communication
Notions	3.3.2. Spécificités de la communication électronique Protection contre les virus et les actes de malveillance.
Présentation	Ce document recense les risques les plus courants : virus, spam, canulars. Ils donne des exemples d'actes de malveillance et fournit des définitions précises. Des solutions sont systématiquement présentées et des conseils sont donnés pour adopter un comportement réduisant les risques.
Pré-requis	L'utilisation courante d'un poste de travail informatique.
Mots-clés	Sécurité, actes de malveillance, virus, spam, canulars, cheval de troie, antivirus, pare-feu
Auteur(es)	Christian Draux
Version	1.0
Date de publication	14 Janvier 2005

Sécurité du poste de travail

Une récente étude du fournisseur d'accès AOL révèle que près des trois quarts des internautes français ont déjà été infectés par un virus informatique. Une autre étude du CLUSIF (Club de la sécurité des systèmes d'information) de juin 2004 montre que 40 % des causes de panne informatique sont dues à des virus.
Il importe donc de pouvoir identifier les différents parasites informatiques, de les prévenir et d'adopter un comportement qui garantisse la pérennité des données dont chacun est responsable.

I - Les dangers potentiels

A – Les virus

Situation 1	Une partie du travail que vous devez réaliser est stocké sur une clef USB appartenant à un autre utilisateur, vous connectez la clef sur votre poste et au moment d'ouvrir le document, le message suivant s'affiche sur votre écran :
	
	1. ***Quel est le type de programme qui vient de déclencher l'ouverture de cette boîte de dialogue ?*** 2. ***De quel danger prévient le message ?*** 3. ***Quelle est la réaction la plus appropriée :*** • ***si l'on souhaite conserver le fichier ;*** • ***si l'on a un doute ;*** • ***si ce fichier vous est totalement inconnu.***

1. Définition
*Un **virus** est un programme informatique, situé dans le corps d'un autre programme qui modifie le fonctionnement de l'ordinateur à l'insu de l'utilisateur.*
Il se propage par **duplication**. Pour cela, il va infecter d'autres programmes d'ordinateur en les modifiant de façon à ce qu'ils puissent à leur tour se dupliquer. Il agit lorsqu'il est chargé en mémoire au moment de l'exécution du logiciel infesté.
La plupart des virus **visent à déclencher une action**. Certaines actions sont sans danger : affichage d'un message, exécution d'une musique, dessin d'une spirale sur l'écran, etc. D'autres ont une action beaucoup plus nuisible.
2. Formes
On distingue les formes suivantes prises par les virus :

Le **virus programme (ou virus d'application)** infecte les programmes exécutables. Il se glisse dans une partie du code et sera exécuté en même temps que l'application. Il en profitera pour se reproduire, contaminer d'autres exécutables et déclencher l'action prédéterminée par son auteur.

Exemple : « Chernobyl (1998).

Le **virus de script** infecte les pages HTML chargées par un internaute. Une page HTML est composée de balises interprétées par le navigateur. Il est possible d'ajouter dans une page HTML des programmes écrits dans un autre langage pour enrichir les pages et les rendre dynamiques. Les plus utilisés sont VB-Script et JavaScript. VB-Script est à l'origine de nombreux virus. Exemple : « I love you (mai 2000) ».
Le **virus macro** est un virus qui infecte des documents (courrier, tableau, etc...). Il est possible d'insérer dans un document des actions programmées pour automatiser certaines tâches : création de formulaires, mises en forme automatisées, etc.. Ces tâches sont réalisées à l'aide d'un langage de programmation (Visual Basic pour Application pour les applications de la suite Office de Microsoft). Le virus se sert de ce langage pour se reproduire et déclencher une action destructrice. Exemple : « Concept (1995) »
Le **virus système** (ou **virus de secteur d'amorce)** infecte les zones systèmes des disques durs ou des disquettes. Ces virus remplacent le secteur d'amorce du disque infecté par une copie de leurs codes. Exemple : « Stoned (1988) », « Form (1991) », « AnticMos (1994) »
Enfin, le **virus de mèl**, également appelés **ver**. Ce virus se sert des programmes de messagerie (notamment Microsoft Outlook et Outlook Express) pour se répandre à grande vitesse, en s'envoyant automatiquement à tout ou partie des personnes présentes dans le carnet d'adresses. Le ver est une variante de virus qui a la particularité de ne pas avoir besoin de support pour se reproduire, il se suffit à lui-même. Exemple : « KakWorm (1999) », « Melissa (1999) » « Happy99 (1999).

3. Signature

Lorsqu'un virus cherche à infecter un nouveau fichier, il commence par vérifier que le virus n'est pas déjà présent dans le fichier, une nouvelle infection pourrait compromettre son efficacité. Il réalise ce contrôle par la recherche d'une séquence de code appelée **signature**.

4. Techniques de dissimulation

Les virus utilisent différentes techniques pour être plus difficiles à détecter par les antivirus :

- **furtifs** : ils interceptent les demandes du système d'exploitation et présentent les informations telles qu'elles étaient avant l'infection, l'objectif est de ne pas être décelé.
- **polymorphes** : ils changent leurs signatures à chaque nouvelle infection de fichier ;
- **rétrovirus** : ils attaquent les antivirus en bloquant leur exécution et leur redémarrage ;
- **hybrides** : ils combinent les caractéristiques de plusieurs familles.

Les virus par email se déguisent en fichier texte, image, son, vidéo ... Un double clic, ou l'ouverture automatique de ces fichiers multimédia, active le virus.

B – Les chevaux de Troie

Situation 2

À l'ouverture de votre logiciel de messagerie vous découvrez le message suivant :
Le message est le suivant :

Client de Microsoft

Voici la dernière version de mise à jour de sécurité « Correctif cumulatif, septembre 2003 », mise à jour qui élimine toutes les vulnérabilités qui affectent MS Internet Explorer, MS Outlook et MS Outlook Express ainsi que trois nouvelles vulnérabilités récentes.

Installez cette mise à jour immédiatement pour préserver la sécurité de votre ordinateur face aux vulnérabilités, la plus importante d'entre elles peut permettre à un pirate d'exécuter des programmes sur votre ordinateur. Cette mise à jour se cumule avec les précédents correctifs.

Remarque : un correctif est un programme qui corrige des dysfonctionnements, bogue ou faille de sécurité, découverts dans un logiciel.

1. ***Quel est l'auteur apparent de ce message ?***

Vous n'avez jamais envoyé de mèl à cet éditeur de logiciels.

2. ***Comment se fait-il qu'il vous envoie un courrier électronique ?***

Ce message est accompagné d'une pièce jointe. La suite du message précise qu'il suffit d'exécuter la pièce jointe et de cliquer sur « **oui** » lorsqu'une boîte de dialogue s'ouvrira pour vous proposer d'exécuter le programme en pièce jointe.

Pris d'un doute vous vous rendez sur un site spécialisé dans la sécurité informatique, le site : http://www.hoaxbuster.com, et vous entrez les premiers mots du message : « this is the latest version of security update, the "September 2003, Cumulative Patch" » sur le moteur de recherche du site.

La première réponse fournie par le site est la suivante :

MISE EN GARDE - **Correctif Microsoft ou simple ver ?**

Si vous avez reçu un e-mail "aux couleurs" de Microsoft vous proposant d'installer un soi-disant correctif détruisez le au plus vite.

Sachez que Microsoft ne distribue jamais de logiciels en pièce(s) jointe(s) par courrier électronique. Il s'agit en réalité d'un nouveau ver qui une fois installé exécutera des **actions dangereuses pour l'ordinateur.**

Vous vous rendez sur le site de l'éditeur de logiciels Microsoft et vous découvrez la page suivante :

http://www.microsoft.com/france/securite/gpublic/protect/politique_emails.aspx

Politique Microsoft de diffusion des mises à jour des logiciels

Pour une informatique sûre et fiable, il est important de ne jamais utiliser de logiciels provenant de sources inconnues.

Comme indiqué dans un avis du CERT, des utilisateurs malveillants emploient souvent des "chevaux de Troie" pour introduire des logiciels pernicieux dans les ordinateurs d'utilisateurs imprudents.

Cheval de Troie

Un cheval de Troie est un logiciel qui, sous l'apparence d'un logiciel utile, réalise en fait de façon cachée des **actions dangereuses pour l'ordinateur infecté**. Par exemple, un pirate peut développer un programme de jeu qui efface délibérément des fichiers sur l'ordinateur qui l'héberge, puis il se propagera via la messagerie de l'utilisateur.

Un autre mécanisme, fréquemment utilisé et qui s'apparente au cheval de Troie, consiste à envoyer par courrier électronique un **programme malveillant**, en annonçant qu'il s'agit d'une mise à jour d'un logiciel et **en se faisant passer pour l'éditeur de ce logiciel**. Récemment, de nombreux courriers de ce type sont apparus sur Internet, annonçant des mises à jour de logiciels Microsoft ou d'autres éditeurs. Il ne s'agit que de **logiciels dangereux** destinés à endommager les fichiers des utilisateurs qui les auraient exécutés.

Sachez que Microsoft ne distribue jamais de logiciels en pièce(s) jointe(s) par courrier électronique

Nous distribuons des logiciels sur des supports physiques comme des **CD-ROM** et des **disquettes**.
Nous distribuons les mises à jour sur Internet **exclusivement** via nos sites Web américain et français, ou via le centre de téléchargement.
Nous envoyons parfois des courriers électroniques à nos clients pour leur **signaler la parution d'une mise à niveau**. Toutefois, ces courriers contiennent **uniquement des liens** vers nos sites de téléchargement ; **nous ne mettons jamais en pièce jointe de logiciels à nos messages**. Les liens mènent toujours vers notre site Web ou notre site FTP.
Nous utilisons toujours Authenticode pour **signer numériquement nos produits**, ce qui permet aux utilisateurs de vérifier qu'ils ont reçu la bonne version.

Si vous recevez un courrier électronique se faisant passer pour Microsoft et contenant un logiciel joint, n'exécutez pas ce logiciel. Supprimez complètement ce message avec sa pièce jointe.
Si vous souhaitez aller plus loin, signalez ce message au fournisseur d'accès Internet (FAI) dont dépend l'expéditeur. De nombreux FAI offrent la possibilité de signaler de tels abus.

3. Quel comportement adopter vis-à-vis du message reçu dans votre boîte aux lettres ?

Définition

Un cheval de Troie est un programme qui se présente sous une forme anodine (mèl, bandeau publicitaire, jeu en téléchargement) mais qui contient en réalité des instructions cachées, dans le but de pénétrer par effraction dans des fichiers pour les consulter, les transférer, les modifier ou les détruire .

Il permet à un pirate de s'introduire dans une machine sans le consentement de l'utilisateur. Dans ce cas, il insère un logiciel "serveur" qui offrira au pirate toutes les informations dont il a besoin. Le pirate pourra prendre le contrôle à distance de l'ordinateur infecté. À la différence d'un virus, il ne cherche pas à se reproduire. L'objectif est de récupérer des informations confidentielles : codes de carte bancaire, identifiant et mots de passe, documents personnels.

Le cheval de Troie est avant tout **un moyen de transport d'un parasite** plus ou moins dangereux. Il utilise souvent une faille de sécurité pour s'introduire dans un ordinateur.

C – Les espiogiciels (spyware)

Définition

Logiciel introduit dans un ordinateur sans l'autorisation explicite de son utilisateur pour collecter des informations et les transmettre à un tiers.

L'objectif des espiogiciels n'est pas de détruire mais d'envoyer des informations à une société ou à une pirate sans se faire remarquer. Ces logiciels sont parfois présentés par des sociétés commerciales comme des outils de suivi des habitudes d'un utilisateur dans le but d'améliorer les produits de la société, mais cette collecte effectuée sans le consentement de l'utilisateur est une intrusion dans la vie privée. On les trouve notamment dans les bandeaux publicitaires de page HTML, dans les logiciels de téléchargement et d'échange de morceaux de musique. Certains sont installés par des chevaux de Troie et peuvent collecter des informations privées comme l'identité, le carnet d'adresses, les mots de passe ou les codes de carte bancaire.

D – Le spam

Situation 3	À l'ouverture de votre logiciel de messagerie vous découvrez le message suivant :

From: "bc1234" < bc1234@fai.com>
To: clambey@fai.fr, ckel@fai.fr, christiane.deschambr@fai.fr, christine.dufond@fai.fr, clambey@fai.fr, ckel@fai.fr
Subject: !cid_yiprtvmv_iwpjxbnd_jwzaesmk
Date: Tue, 26 Oct 2004 13:24:00 -0300

	En observant les différents éléments qui composent l'en-tête de ce message (expéditeur, destinataire, sujet), précisez quels sont les éléments qui vous permettent de penser que ce message est suspect ?

1. Définition

Le spam (ou pourriel) est un courrier électronique abusif et indésirable.

Le spam se réfère aux courriers électroniques publicitaires envoyés en masse à des milliers d'internautes qui n'ont pas donné leur accord pour les recevoir. On surnomme les émetteurs de ces messages « **spammeurs** ».

2. Intérêt de cette pratique pour les expéditeurs

Il s'agit d'un procédé très peu coûteux pour expédier des offres commerciales à des millions d'adresses. Des logiciels spécialisés appelés « robots » parcourent le Web pour y récupérer les adresses. L'envoi des courriels est quasiment gratuit. Le taux de retour est extrêmement faible mais suffisant.

3. Les inconvénients

Le spam présente deux inconvénients majeurs. Il parasite Internet, en monopolisant plus de 50 % du trafic du courrier électronique, et dévalorise les démarches commerciales responsables sur Internet. Les acteurs de l'Internet s'efforcent donc de limiter le phénomène par des moyens techniques, et les États tentent d'y mettre fin par des dispositions législatives. Mais l'aspect international du phénomène et l'inventivité des spammeurs rendent l'éradication du fléau très difficile.

E – les canulars

Situation 4	Parmi les messages reçus, vous découvrez celui-ci expédié par un(e) ami(e).

Sujet: Vol de voiture

On n'est jamais trop prudent.
SOYEZ ATTENTIFS TOUT LE MONDE ! Soyez avisés qu'une nouvelle façon de voler une voiture est en opération. (Ceci peut aussi être employé comme complot pour ravir quelqu'un)

Imaginez: Vous marchez dans le stationnement, déverrouillez votre auto et montez. Vous verrouillez toutes les portes, démarrez et embrayez pour reculer et soudain, vous regardez dans votre miroir pour reculer de votre espace de stationnement et vous remarquez un morceau de papier collé dans votre vitre arrière. Vous remettez la transmission à PARK, déverrouillez les portes et sortez de l'auto pour retirer ce morceau de papier (ou ce que c'est) qui obstrue votre vue. Lorsque vous êtes derrière l'auto c'est là qu'apparaissent les voleurs d'on ne sait où, qui sautent dans votre auto et partent !!! Votre moteur tournait (les dames auraient leur sac à main dans l'auto) et en plus ils vous passent presque sur le corps lorsqu'ils partent en vitesse avec votre auto. SOYEZ AVISÉS DE CE "NOUVEAU" STRATAGÈME QUI EST MAINTENANT UTILISÉ. Faites seulement partir et enlevez ce damné papier collé à votre vitre plus tard et soyez fiers d'avoir lu ce courriel. J'espère que vous le ferez parvenir à tous vos amis et votre famille SPÉCIALEMENT AUX FEMMES ! Un sac à main contient toutes vos identifications et vous ne voulez certainement pas que ces gens aient votre adresse à la maison. ILS ONT DÉJÀ VOS CLEFS !!!

1. ***À la lecture du contenu du message, peut-on deviner dans quelle langue initiale a été écrit ce message ?***
2. ***Quel est l'objectif poursuivi par son initiateur ?***

1. Définition

Un canular (en anglais hoax) est une annonce reçue par mèl qui incite à transférer ce message à tous les contacts contenus dans le carnet d'adresses.

Ce procédé a pour but l'engorgement des réseaux ainsi que la désinformation.

2. Variété des canulars

- **Arrivée d'un danger :** le message prévient d'un danger, l'arrivée d'un nouveau virus (faux virus), il se sert de la caution de sociétés renommées pour appuyer ces affirmations.
- **Les chaînes de solidarité** : il encourage à sauver une ou plusieurs personnes atteintes d'une maladie rare, il fait appel à la générosité des internautes.
- **Un gain potentiel** : le message promet de gagner beaucoup d'argent en très peu de temps. Le message est parfois étayé d'un exemple extravagant (gagner plusieurs milliers de dollars).
- **Bonne ou Mauvaise fortune** : Le message vous prévient de la bonne fortune ou du malheur le plus terrible si vous ne le faites pas suivre. On cite l'exemple d'une personne qui n'a pas renvoyé le message et qui a eu tous les malheurs du monde jusqu'à ce qu'elle se décide, ses problèmes se sont alors tous immédiatement résolus.

- **Désinformation**
  Le message "prévient" d'un fait généralement scandaleux et vise à faire réagir le destinataire et réclame la diffusion la plus large possible.

II – Les modes de contamination

Pour pouvoir se propager, les parasites informatiques ont besoin d'utiliser des supports physiques.

A - Les supports amovibles

Tout support qui a besoin d'être connecté ou introduit dans un ordinateur est un danger potentiel.

- **La disquette** : support le plus ancien, la disquette permet de sauvegarder les fichiers d'un ordinateur puis de les restaurer sur un second. Si les fichiers de la première machine sont infectés par un virus, la copie sur la disquette copiera le virus qui se retrouvera ensuite sur le second poste. Les disquettes de forte capacité (Zip) sont aussi susceptibles de transmettre des virus.
- **Le CD-ROM** : support de plus grande capacité, on y trouvait au début des programmes vendus par les éditeurs de logiciels ou insérés gratuitement dans une revue informatique. Certains programmes comportaient des virus. Aujourd'hui les CD-ROM et DVD-ROM sont devenus inscriptibles ou réinscriptibles et deviennent un facteur de propagation identique aux disquettes.
- **La clef USB**. Il s'agit d'une mémoire réinscriptible de capacité plus élevée Elle remplace la disquette et peut aussi contaminer un ordinateur.

B - Le réseau informatique

La plus grande partie des infections est réalisée aujourd'hui par les réseaux.

- **Réseau interne** : une seule machine infectée transmet par le réseau le parasite à l'ensemble des ordinateurs.
- **Réseau Internet** : la messagerie électronique, que ce soit par un message au format HTML ou une pièce jointe va permettre de diffuser le parasite en utilisant des adresses de destinataires contenues dans le carnet d'adresses de l'ordinateur. La contamination sera d'autant plus rapide que les utilisateurs utiliseront leur messagerie et répondront à des sollicitations dangereuses. Certains parasites n'ont pas besoin de la messagerie, ils se transmettent à l'aide des messages d'information que se transmettent les ordinateurs pour communiquer.

III – Les dommages

Si certains parasites sont inoffensifs, d'autres ont un comportement beaucoup plus nuisible et préjudiciable pour les données et parfois pour la machine elle-même.

- **Destruction de fichiers** : elle peut être partielle en s'attaquant à un type de fichiers (programme, document, image, son) ou totale lors d'un formatage du support.
- **Corruption de fichiers** : l'objectif est de modifier la structure du fichier pour le rendre inutilisable :caractères parasites dans un document, son inaudible, images dégradées, programme inutilisable. Lorsqu'il s'agit de données de gestion, le coût pour une organisation peut être très élevé.
- **Destruction matérielle** : certains virus vont exécuter des instructions à répétition pour provoquer un échauffement qui détruira un composant ou bien détruire le programme qui gère les entrées-sorties d'information (BIOS) de la carte mère d'un ordinateur. L'appareil est détruit sans savoir s'il s'agit d'une panne matérielle ou d'un acte volontaire de destruction.
- **Instabilité du système** : d'autres virus rendent le système instable par un blocage aléatoire qui oblige à redémarrer l'ordinateur.
- **Dégradation des ressources du système** : le virus utilise les ressources de l'ordinateur (mémoire, disque dur) pour se répliquer, il ralentit le système jusqu'au blocage complet par saturation des disques ou de la mémoire.

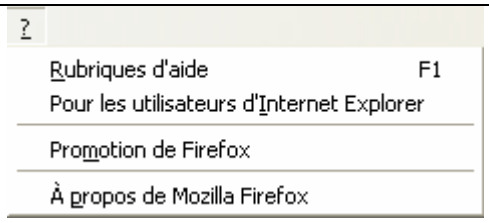
- **Compromission des paramètres de sécurité** : il s'agit d'une action courante des chevaux de Troie qui installe des modules pour intercepter les frappes au clavier (KeyLogger) notamment les mots de passe et les envoyer vers une machine à l'extérieur du réseau.
- **Blocage de la sécurité :** le virus s'attaque aux programmes anti-virus ou pare-feu en les désactivant pour les empêcher de fonctionner.

IV - La prévention

La prévention passe par une protection du poste de travail. Elle forme un tout. S'il manque un élément, c'est la sécurité complète de l'ordinateur qui peut être compromise. Lorsqu'un poste de travail appartient à un réseau important c'est le rôle de l'administrateur réseau de garantir la sécurité des machines et des données. Sur de petits réseaux (cas des PME ou des petites structures) ou sur un poste isolé c'est à l'utilisateur de prendre en charge cette protection.

A – La mise à jour des programmes

Comment connaître la version de son système d'exploitation ou d'un logiciel ?

<table>
<tr>
<td> 
</td>
<td>La plupart des logiciels disposent sur la première ligne de leur menu d'un « ? » qui permet d'accéder à l'aide. La dernière ligne de ce menu propose une rubrique « À propos », il suffit de cliquer sur cette ligne pour voir apparaître une boîte de dialogue qui fournit des informations sur le logiciel utilisé.</td>
</tr>
<tr>
<td> 
</td>
<td>Il s'agit ici d'un navigateur Internet « Firefox » dans sa version 1.0.
Lors de la recherche d'une mise à jour sur Internet, on choisira d'éventuelles mises à jour pour ce produit.
Pour connaître la version du système d'exploitation, il faut ouvrir l'explorateur et cliquer sur « ? »</td>
</tr>
</table>

Beaucoup de programmes comportent des bogues ou des failles de sécurité dont se servent les parasites pour se propager et infecter les ordinateurs. Les mises à jour concernent aussi bien le système d'exploitation que les programmes applicatifs.

1. Le système d'exploitation

On trouve sur les postes de travail 3 grandes familles de système d'exploitation. Deux systèmes propriétaires OS-Mac de la société Apple, Windows de la société Microsoft et une famille de systèmes basés sur Linux.

La course à des produits toujours plus performants conduit les éditeurs à mettre sur le marché de nouveaux systèmes d'exploitation ou de nouvelles versions insuffisamment testés. Très rapidement des failles de sécurité sont découvertes qui entraînent la publication de correctifs. Lorsqu'une machine n'est pas à jour de ces correctifs elle devient une cible potentielle pour tout type d'attaque.

Il est donc impératif de mettre à jour le système d'exploitation. Cette mise à jour peut être manuelle ou automatisée (cf : côté labo – protéger son poste de travail).

2. Les logiciels applicatifs

Les navigateurs Internet, les clients de messagerie et les logiciels métiers comportent eux aussi des failles de sécurité. Leur correction obéit aux mêmes principes que le système d'exploitation.

B – Les logiciels de protection

Pour protéger son poste, il importe de disposer de logiciels qui vont empêcher toute action nuisible et éventuellement neutraliser un programme dangereux. Les principaux logiciels utilisés sont :

1. L'anti-virus

a. Définition

Programme qui empêche les virus de contaminer un ordinateur.

Il peut parfois, pas toujours, neutraliser un virus déjà présent. Le rôle essentiel d'un anti-virus est d'interdire l'arrivée d'un virus dans la machine. Si le virus a réussi à pénétrer à l'intérieur du système, l'action de l'anti-virus sera beaucoup moins efficace. Il faudra alors recourir à un antidote que l'on télécharge sur le site d'un éditeur d'anti-virus ou sur des sites spécialisés dans la sécurité.

b. Efficacité

Pour être efficace un anti-virus doit

- **être présent sur la machine** avant toute source de contamination ;
- **être à jour** : base anti-virale et moteur de détection ;
- **être actif en permanence**.

c. Fonctionnement

Dés qu'un virus tente de pénétrer dans l'ordinateur, l'anti-virus va, en fonction du type de danger :

- **supprimer** (nettoyer) la partie du code correspondant au virus dans le fichier infecté, le fichier pourra alors être normalement utilisé.
- **supprimer le fichier infecté** si celui-ci ne peut pas être nettoyé ou si l'intégralité du code est néfaste;
- **mettre en quarantaine le fichier infecté**, c'est-à-dire déplacer le fichier dans un emplacement contrôlé par l'anti-virus pour l'empêcher de se déclencher.

Ces actions peuvent être automatisées en fonction des réglages du logiciel. Il est donc préférable de vérifier dés l'installation les paramètres par défaut et d'adapter les actions du logiciel en fonction de la politique de sécurité que l'on souhaite implanter sur l'ordinateur. Les logiciels sont très souvent prudents dans leurs actions

d. Technologie

Les anti-virus utilisent différentes technologies pour rechercher les virus :

- **La recherche de signatures**. Le logiciel analyse les fichiers pour détecter la présence d'un virus. Pour que cette méthode soit efficace il faut que la base des signatures soit régulièrement mise à jour. Cette méthode ne permet pas de détecter les virus qui utilisent une nouvelle signature, mais la rapidité (quelques heures) de réaction entre la découverte d'un nouveau virus et la mise à jour de la base permet d'arrêter la plupart des virus.
- **La méthode heuristique** : elle consiste à chercher des instructions suspectes à l'intérieur des fichiers en se basant sur des règles générales de reconnaissance des virus. Cela permet de détecter aussi bien des virus connus qu'inconnus, sans effectuer de fréquentes mises à jour. Toutefois, cette méthode génère parfois de fausses alertes. L'utilisateur doit être capable de faire la différence entre les vraies et les fausses alertes.
- **Le contrôle d'intégrité** : lors de son installation, l'antivirus crée une base de données de tous les fichiers présents sur la machine basée sur la longueur des fichiers et d'autres paramètres. Toute modification d'un fichier fera l'objet d'une alerte.

Les logiciels antivirus combinent ces méthodes pour proposer les produits aussi performants que possible.

2. Le pare-feu

a. Définition

Un pare-feu (firewall en anglais), est un logiciel permettant de protéger un ordinateur des intrusions provenant d'un réseau.

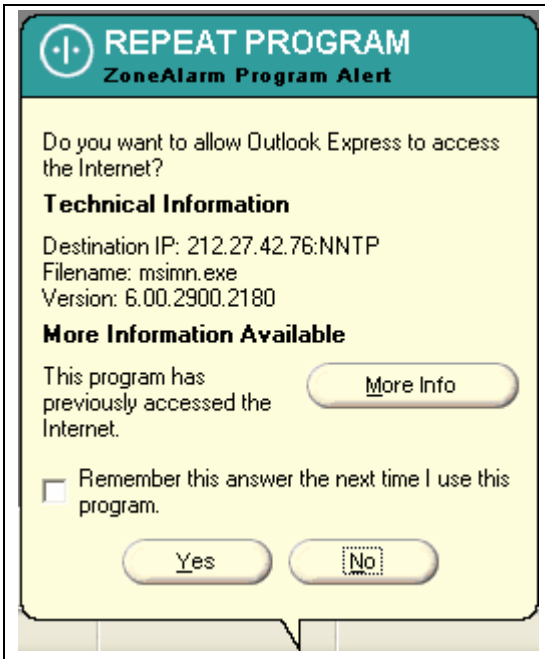
b. Les attaques externes.

Il doit protéger aussi bien le poste des attaques provenant d'Internet que celles provenant d'un réseau interne.

c. Les menaces des logiciels internes

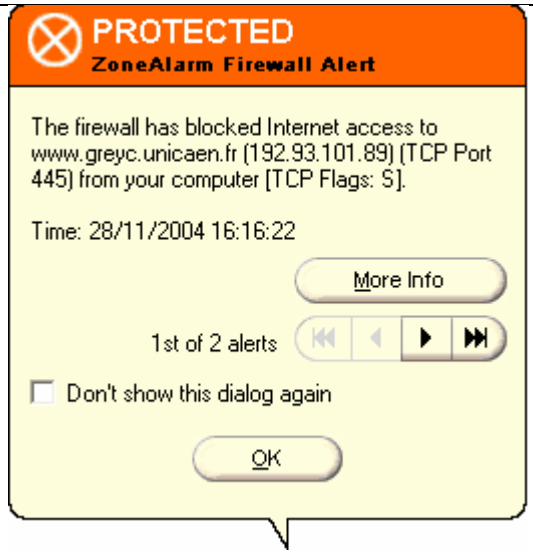
Le pare-feu doit empêcher certains logiciels comme les chevaux de Troie d'entrer en contact avec d'autres ordinateurs situés dans un réseau local ou sur Internet et de leur fournir des informations présentes sur l'ordinateur.

Situation 5 On vient d'installer sur votre poste un pare-feu et au moment de lancer votre logiciel client de messagerie les messages suivant apparaissent :



Le message précise : « Autorisez vous Outlook Express à accéder à Internet ? »

1. ***Que faut il répondre ?***
2. ***Que faut-il faire pour que la question ne soit pas posée à chaque utilisation de ce logiciel ?***



Le message précise : « Le pare-feu a bloqué l'accès Internet au site www.greyc.unicaen.fr (192.93.101.89) (Port TCP 445) depuis votre ordinateur »

1. ***S'agit-il d'une attaque en provenance de l'extérieur ou bien d'un programme présent sur le poste qui tente d'accéder à une autre machine située sur Internet ?***
2. ***Que faut-il faire pour ne plus voir apparaître ce message tout en restant protégé ?***

IV - Dix mesures pour sécuriser son poste de travail

A - Prévenir

Il n'existe pas de système informatique complètement sécurisé mais quelques mesures simples permettent d'éloigner le risque de perdre tout ou partie des données dont on a la responsabilité. En adoptant un comportement responsable, on évitera deux écueils : le laisser-faire et la paranoïa.

1. Sauvegarder ses données.

Cette première mesure est une protection contre les parasites et les autres risques : pannes matérielles, vol, malveillance interne, accident, etc …
Pour être efficace les sauvegardes doivent remplir plusieurs conditions :

- être régulières, le rythme est fonction de l'importance des données et de leurs modifications.
- être réalisées sur un support fiable : bande magnétique, disque dur externe, CD non réinscriptible. Les disquettes Zip et clefs USB sont considérées plus comme un moyen de transport que comme un outils d'archivage. Les CD réinscriptibles offrent moins de fiabilité que les gravures définitives.
- être stockées dans un endroit différent de celui où est situé le poste de travail.

2. Installer et activer un pare-feu.

Toute machine connectée au réseau Internet est susceptible de recevoir la visite d'un pirate ou d'un robot à la recherche d'une nouvelle victime.
Si le système d'exploitation présent sur la machine dispose d'un pare-feu, on vérifiera qu'il est bien installé et actif.
Si le pare-feu présent d'origine n'est pas satisfaisant ou bien s'il n'en existe pas il faudra procéder à son installation.
Il existe des solutions gratuites téléchargeables sur Internet (cf. Webographie), d'autres sont intégrées dans des solutions complètes de sécurisation du poste : antivirus, pare-feu, sauvegardes.

3. Mettre à jour son système d'exploitation et ses applications.

La plupart des programmes comportent des failles de sécurité ou des bogues et les parasites se servent de ces insuffisances pour se propager et déclencher l'action pour laquelle ils sont conçus.
Les éditeurs publient régulièrement des mises à jour qui viennent corriger ces défauts. Il est donc important d'installer ces correctifs.
Mise à jour du système d'exploitation.
Sur les systèmes d'exploitation récents, celle-ci doit être automatisée lorsque le système le permet.
Sur les systèmes plus anciens, c'est à l'utilisateur de faire la démarche qui s'impose pour mettre à jour son système.
Mise à jour des logiciels applicatifs.
La propagation des parasites s'effectue le plus souvent lors de l'utilisation du navigateur Internet, du client de messagerie ou de la messagerie instantanée. Les mises à jour peuvent être couplées avec le système d'exploitation lorsqu'il s'agit du même éditeur ou bien réalisées séparément sur le site Internet de l'auteur du logiciel.
Les logiciels les plus récents comportent, comme le système d'exploitation, une procédure de mise à jour automatisée, il faut vérifier que cette possibilité est active.

4. Installer et activer un anti-virus.

Aucun système d'exploitation ne comporte pour le moment d'anti-virus intégré. Plusieurs solutions sont envisageables : installer un anti-virus gratuit, installer une solution complète de protection proposée par plusieurs éditeurs, utiliser une solution de protection offerte par le fournisseur d'accès Internet auquel on est abonné.
Quelque soit la solution retenue, une fois le logiciel installé, il faudra lancer une recherche anti-virale manuelle, régler la fréquence des recherches anti-virales et les actions à entreprendre en cas d'infection.
Enfin vérifier la périodicité des mises à jour.

5. Installer et activer un anti-espiogiciels.

La plupart des logiciels ne disposent pas d'une protection contre les espiogiciels. Il est donc nécessaire de s'en procurer un et de le paramétrer sur le même principe que l'anti-virus.

6. Filtrer le spam
Les filtres anti-spam servent à distinguer parmi les messages reçus ceux qui comportent un expéditeur connu et ceux qui polluent les boîtes aux lettres.
Ils peuvent être intégrés dans le client de messagerie (Outlook 2003, Mozilla Thunderbird) ou bien installés en plus du client de messagerie. Ils nécessitent souvent un apprentissage, laborieux au début, mais profitable sur le long terme.

Toutes ces mesures visent à protéger le poste informatique des infections externes, mais le comportement de l'utilisateur joue un rôle non négligeable pour prévenir les désagréments liés aux parasites.

B - Adopter un comportement sans risque
Quelques mesures simples permettent à un utilisateur d'éviter d'être une cible potentielle.

7. Ne pas diffuser inutilement son adresse sur Internet.
Lorsqu'on reçoit du spam, c'est que l'adresse que l'on possède circule sur le réseau Internet.
Des programmes malveillants parcourent en permanence les pages HTML visibles sur le Web à la recherche d'adresses de messagerie. Or une adresse peut apparaître sur une page Web à différentes occasions : la signature d'un article, une contribution dans un forum, la saisie dans un formulaire, un annuaire public. L'adresse peut être vendue par un webmestre indélicat
Votre adresse peut figurer dans le carnet d'adresse d'un correspondant, si celui-ci est infecté par un virus ou un espiogiciel.
Pour toutes ces raisons, il est préférable d'utiliser un compte de messagerie dédié aux activités exposées et conserver une autre adresse pour les échanges professionnels ou personnels. Lorsque l'adresse exposée recevra trop de messages indésirables, il suffira de la supprimer et d'en créer une autre. On utilisera des adresses gratuites ou jetables afin de ne pas exposer son propre fournisseur d'accès.

8. Ne pas répondre à un expéditeur inconnu.
Une bonne part des messages non désirés provient d'éditeurs de logiciels, de constructeurs informatiques, d'organismes officiels, il s'agit en réalité d'adresses usurpées dont le véritable expéditeur cherche à contaminer une machine. Parfois il arrive que l'expéditeur soit une personne connue dont l'adresse est falsifiée, le nom de l'expéditeur est connu mais le fournisseur d'accès Internet n'est pas le bon. Il faut s'intéresser au contenu du message qui est très souvent en complet décalage avec la personne sensée avoir expédié le message. Lorsqu'une pièce jointe accompagne le message, il faut s'assurer qu'elle est explicitement déclarée dans le message et en rapport avec l'activité de l'expéditeur.

9. Ne jamais transférer un message à tout son carnet d'adresses
Cette pratique encouragée par le spam est à proscrire absolument. Elle encombre la messagerie, elle divulgue à chacun l'intégralité de vos correspondants. Il est inutile d'envoyer à un correspondant amical ou familial, ces adresses professionnelles, le contraire est aussi vrai.
Il est possible de transférer à certaines personnes un message reçu si ce message présente un intérêt pour elles, mais il est bon de vérifier avant qu'il ne s'agit pas d'un canular. Une recherche sur des sites spécialisés comme www.hoaxbuster.com ou www.secuser.com/hoax, peut éviter d'être piégé et parfois de se rendre ridicule.

10. Régler soigneusement son client de messagerie.
Une maîtrise sérieuse de son logiciel de messagerie permet de canaliser le flot des messages en croissance régulière. Des règles anti-spam permettent d'envoyer dans un dossier réservé tous les messages filtrés, une observation régulière de son contenu lève le doute sur certains messages.
L'utilisation de règles de filtrage sur l'expéditeur, l'objet, le contenu permet de classer son courrier dans des dossiers prévus à l'avance, il ne reste plus que quelques messages dans la boîte de réception sur lesquels il sera plus facile de prendre une décision.
Certains messages sont écrits en HTML, ils sont plus attrayants mais potentiellement plus dangereux, on pourra régler dans les options la lecture « en texte brut » afin d'éviter une contamination par un code malveillant.