Formation au C2i®

B3

Sécuriser, sauvegarder, archiver ses données en local et en réseau filaire ou sans fil

Auteurs :

Alain Berro

David Panzoli

Nathalie Valles-Parlangeau

Université Toulouse 1 Sciences Sociales

Module développé dans le cadre du projet CIIMES 2005,
Certification Informatique et Internet
Mutualisée pour l'Enseignement Supérieur

Edition : CIIMES, www.ciimes.org
Scénarisateur : Vincent Buous
Version : 1.0

SOME RIGHTS RESERVED

Publié sous Licence Creative Commons "By-NonCommercial-ShareAlike"
- http://creativecommons.org/licences/by-nc-sa/2.0/ -
Remarque importante : "Vous n'avez pas le droit d'utiliser ce document à des fins commerciales sans l'autorisation préalable de l'auteur"

Septembre
2005

Table des matières

Introduction **7**

Chapitre I. Se protéger de la perte de données **9**

Objectifs pédagogiques 9

Partie A. Assurer la protection de sa machine 9

1. Le mot de passe 10
2. Le pare-feu (firewall) 12

Partie B. Assurer la protection contre les virus 12

Définition d'un virus 12

1. Les différents types de virus 13
2. Comment en guérir ? 14
3. Prévention et prudence 15
4. Principaux réglages d'un antivirus 16

Partie C. Prévenir la perte de données 16

1. Paramétrer correctement sa corbeille 17
2. Surveiller le bon état de votre machine 17
3. Assurer une sauvegarde 18

Partie D. Exercices - QCM 18

Exercice n°1. Assurer la protection de sa machine 18

Exercice n°2. Assurer la protection contre les virus 18

Exercice n°3. Assurer la protection de sa machine - Questions 20

Exercice n°4. Assurer la protection contre les virus - Questions 20

Chapitre II. Se protéger de la malveillance **23**

Objectifs pédagogiques 23

Partie A. Assurer la protection contre des mouchards (spyware) 24

Les spywares 24

1. Les différents types de spywares 24

2. Lutter contre les spywares. 25
Partie B. Prévenir la malveillance. 26
Se protéger de la malveillance. 26
1. Protéger un fichier. 26
2. Crypter un fichier. 29
Partie C. Exercices - QCM. 34
Exercice n°5. Associer un mot de passe à un document (Windows, Excel). 34
Exercice n°6. Questions. 34
Chapitre III. Se préserver des nuisances. 37
Objectifs pédagogiques. 37
Partie A. Les pourriels ou spams. 37
Définition des pourriels. 37
1. Lutter contre le spam. 39
2. Arnaques et escroqueries. 40
Partie B. Les canulars (hoax). 42
Définition des hoax. 42
1. Exemples de canulars. 42
2. Stop aux canulars !. 43
Partie C. Exercices - QCM. 44
Exercice n°7. Info ou intox ?. 44
Exercice n°8. Questions. 44
Chapitre IV. Détecter un comportement anormal. 47
Objectifs pédagogiques. 47
Partie A. Comportement de la machine ou des périphériques. 48
Comportement de la machine ou des périphériques. 48
1. Réplication des vers ou des virus. 48
2. Propagation des vers ou des virus. 50
Partie B. Fonctionnement anormal des logiciels. 51
Préambule. 51
1. Prise de contrôle de l'ordinateur. 51
2. Détournement. 52
Partie C. Exercices - QCM. 52
Exercice n°9. Questions. 52

Chapitre V. Assurer une sauvegarde (sur le réseau, support externe,...) 55

Objectifs pédagogiques 55

Partie A. Pourquoi, quand, quoi, ... ? 55

1. Pourquoi faire une sauvegarde ? 55
2. Quelle fréquence de sauvegarde ? 56
3. Que doit-on sauvegarder ? 56

Partie B. Des méthodes de sauvegarde 56

1. Simple copie sur support amovible 56
2. Le mirroring 58
3. Le backup 59

Chapitre VI. Compresser/décompresser ses données 61

Objectifs pédagogiques 61

Partie A. Introduction 61

Définitions 61

1. Pourquoi a-t-on besoin de compresser les données ? 62
2. La taille des fichiers 62

Partie B. Compresser et décompresser un fichier et/ou un répertoire 63

Définitions 63

1. Création d'une archive avec Winzip 64

Partie C. Les divers formats de compression (zip, rar, gzip, tar, ...) 65

1. Formats de compression : définitions 65

Partie D. La compression des images, du son et des vidéos 65

Définitions 65

1. Les formats d'images 66
2. Les formats audios 69
3. Les formats vidéos 70

Partie E. Exercices - QCM 71

Exercice n°10. Compression et Archivage 71

Exercice n°11. L, tu prends trop de place ! 71

Exercice n°12. Questions 72

Chapitre final 75

Glossaire 77

Préambule

Introduction

Les objectifs de ce module sont d'apprendre :

- à se protéger de la perte de données, de la malveillance et des nuisances d'Internet
- à détecter un comportement anormal de votre environnement matériel et logiciel afin de déceler la présence d'un virus, d'un logiciel malveillant...
- à sauvegarder et compresser ses données

Implication :
Ce module demande à l'apprenant de faire preuve de réflexion et d'esprit de synthèse. Les outils pouvant être abordés dans ce chapitre étant divers et variés, l'apprenant sera préparé à les utiliser mais ne pourra pas les manipuler tous dans le cadre de ce cours.
Temps d'apprentissage :
Cours et exercices 3h30 minimum
Difficulté :
Intermédiaire
Pré-requis :
Module B1 - S'aproprier son environnement de travail.
Modalités d'évaluation :
A la fin de chaque item de ce chapitre, sont proposés des exercices pratiques, des questions ouvertes et des QCM.

Chapitre

I

Se protéger de la perte de données

Objectifs pédagogiques

La perte de données peut être provoquée par un virus, un effacement intentionnel de la part d'un autre utilisateur, un écrasement ou effacement accidentel de la part de l'utilisateur lui-même ou bien une panne matérielle (par exemple : une panne de disque dur).

Le but de ce chapitre est que l'apprenant puisse :

- Identifier et évaluer les risques de perte de données de son environnement.
- Savoir se protéger de la perte de données.
- Agir de manière préventive.



Conseil
Mieux vaut prévenir que guérir.

Nous verrons dans un premier temps comment protéger sa machine puis comment se protéger des virus et pour terminer comment prévenir la perte de données.

Partie A. Assurer la protection de sa machine

L'intrusion d'un autre utilisateur peut se faire soit par une prise en main directe de votre machine soit en passant par votre connexion réseau.
Ces deux points ont une réponse spécifique qui sont respectivement l'utilisation d'un mot de passe et d'un pare-feu.

1. Le mot de passe

Actuellement tous les systèmes d'exploitation permettent à chaque utilisateur de protéger son espace de travail à l'aide d'un mot de passe de connexion associé à un nom de connexion (login). En plus de procurer une sécurité cela permet de créer un profil pour chaque utilisateur. Ce dernier peut ainsi personnaliser son espace de travail comme il le souhaite.

Lorsque vous possédez un compte sur un ordinateur, le seul et unique contrôle d'accès à cette machine est en général votre mot de passe. Si quelqu'un craque celui-ci (voir la définition du glossaire : craquer (un mot de passe), il pourra ensuite travailler sur votre machine et en empruntant votre nom (éventuellement sans que vous ne vous en aperceviez), lire tous vos fichiers (courriers, textes...), détruire ces fichiers ou plus insidieusement en modifier certains. Cette fonction essentielle du mot de passe est devenue encore plus importante avec l'utilisation des réseaux et d'Internet.



Attention
Craquer un mot de passe est d'autant plus aisé que celui-ci aura été mal choisi.

♦ **Comment puis-je craquer votre mot de passe ?**

Tout d'abord, je regarderai si vous n'avez pas noté ce mot de passe. Je chercherai ainsi sur ou sous votre clavier, derrière l'écran et dans votre agenda. Puis j'essaierai, comme mot de passe, les informations personnelles vous concernant dont je dispose : identifiant, prénom, numéro de téléphone, prénoms des enfants, date de naissance, adresse, etc. Si ça ne marche pas, je tenterai alors des combinaisons avec tout ça : première syllabe des prénoms des enfants, numéro de téléphone inversé.

Si cette méthode artisanale mais souvent efficace échoue, j'automatiserai la recherche avec un programme pour craquer les mots de passe. Ces programmes utilisent des dictionnaires de mots de passe ou tout simplement effectuent une recherche à l'aide d'un générateur aléatoire.



Attention
Si votre mot de passe est simple et court, il sera vite craqué !

♦ **Ce qu'il ne faut pas faire !**

- Il ne faut pas noter son mot de passe, choisissez donc un mot de passe facile à mémoriser.
- Il faut le garder secret. Si l'on désire travailler à plusieurs sur un même ordinateur, il faut créer autant de comptes que d'utilisateurs.
- Il ne faut pas choisir comme mot de passe une information personnelle (prénom, nom du projet...). Les mots présents dans un dictionnaire français ou étranger sont à éviter et à proscrire également toute variation de ce qui précède (ajout de chiffres, mots accolés, ...).
- Ne pas utiliser le même mot de passe pour tous ses besoins (accès machine, courrier, ftp, ...)

♦ **Comment choisir votre mot de passe ?**

- Utiliser un mot de passe suffisamment long : huit caractères est un minimum.
- Mélanger les différents types de caractères : lettres minuscules, majuscules, chiffres, ponctuation, caractères spéciaux.
- Etre imaginatif.

Il faut par ailleurs changer son mot de passe régulièrement, même s'il est très bon, tout simplement à cause du risque d'interception sur le réseau ou sur votre ordinateur. La fréquence de changement dépend de l'utilisation que vous faites de l'informatique et de votre environnement. Mieux vaut cependant changer son mot de passe moins souvent que de l'oublier.



Conseil

Entre longueur et complexité, privilégier un mot de passe long de faible complexité, il sera facile à retenir pour vous et difficile à craquer.



Exemple

Le mot de passe *#!$d@[* est difficile à retenir et facile à craquer car relativement court.

Par contre *jsisueseignanthureux* est facile à retenir. Regardez bien vous devriez trouver la phrase utilisée et la technique de cryptage. Ce mot de passe est par contre beaucoup plus difficile à craquer que le précédent car il est très long.

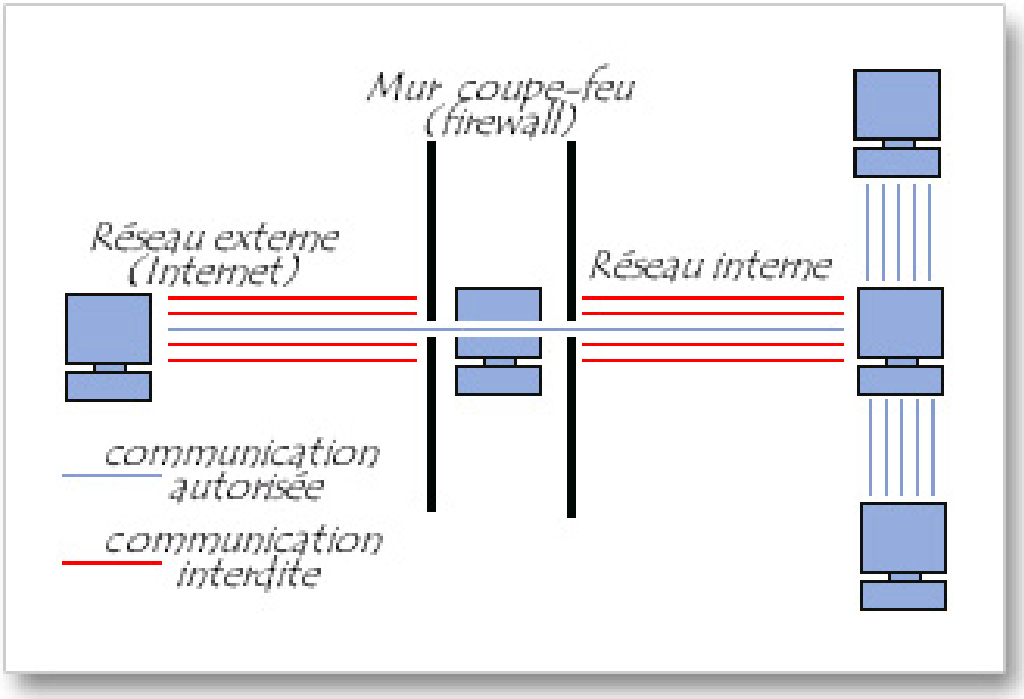


Démarche

Changement de mot de passe sous Windows XP :

Lancer la fenêtre Démarrer/Paramètres/Panneau de configuration/Comptes Utilisateurs Choisissez votre nom d'utilisateur Puis l'action " Changer de mot de passe "

2. Le pare-feu (firewall)



▲ IMG. 1

A l'aide du firewall l'utilisateur peut définir sa politique de sécurité :

- Soit il autorise uniquement les communications ayant été explicitement autorisées donc *tout ce qui n'est pas explicitement autorisé est interdit.*
- Soit il empêche les échanges qui ont été explicitement interdits donc *tout le reste est autorisé*.

  La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication. En effet, chaque fois que le firewall détecte un échange jamais rencontré jusqu'ici, il demande à l'utilisateur d'autoriser ou d'interdire cet échange.

Partie B. Assurer la protection contre les virus

Définition d'un virus

Les virus forment le danger numéro 1 sur Internet.



Virus
Un virus informatique est un logiciel malveillant écrit dans le but de se dupliquer sur d'autres ordinateurs.
Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté.
Il peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les disquettes, les cédéroms, les clefs USB etc.

1. Les différents types de virus

La seule classification possible des virus est d'ordre technique tant les buts recherchés par leurs auteurs sont divers. Le point commun à tous les virus est leur méthode d'intrusion. Ils exploitent des failles de sécurité du système d'exploitation, d'un programme réseau (serveur FTP, client de messagerie instantanée, etc.) ou simplement de l'utilisateur.

Le virus se présente sous la forme d'un morceau de code parasite qui s'insère dans un programme. L'exécution du programme hôte déclenche l'exécution du virus. Lors de son exécution, le virus, à l'instar de son homonyme biologique, cherche avant tout à se propager (se reproduire) et ensuite à effectuer la tâche pour laquelle on l'a programmé.
Les raisons pour lesquelles on programme un virus sont très différentes. Certains sont relativement inoffensifs (exemple : affichage de messages d'erreurs) alors que d'autres peuvent aller jusqu'à détruire la totalité des données présentes sur la machine infectée. Ils peuvent également servir pour détourner des ressources : on parle alors de machines " zombies ", destinées à servir de support à des opérations illicites.

Les TSR (Terminate and Stay Resident) ou virus d'application

Par le terme virus on désigne par défaut les *virus d'application* qui sont historiquement les premiers. Ils exploitent des failles de sécurité du système d'exploitation et utilisent des fichiers exécutables comme hôtes d'accueil. Leur nom vient du fait qu'ils se terminent rapidement sans causer de dommages visibles (Terminate), mais restent en mémoire vive (Stay Resident) afin d'infecter silencieusement tous les programmes de la machine. Ils ne se propagent pas de manière autonome par le réseau mais sont transmis en même temps que les utilisateurs transmettent les programmes qu'ils parasitent (copie sur disquette, cd-rom, envoi par courrier, etc.).

Certains TSR sont également qualifiés de *bombes logiques* quand ils sont destinés à se déclencher à une date précise. La propagation est initiée quelque temps avant la date prévue afin de maximiser le nombre de machines vérolées qui vont déclencher l'action prévue, mais assez tard pour que le virus ne soit pas découvert et éradiqué avant la date fatidique.

Les vers (worms) ou virus réseaux

Parallèlement à l'explosion des réseaux, Internet en tête, est apparu un nouveau type de virus : le ver. Il fonctionne de façon similaire au TSR mais avec la faculté de se répandre sur un réseau de façon autonome, soit en exploitant des failles de logiciels réseau (messagerie, ftp, etc.), soit en exploitant la " faille utilisateur ". Dans ce cas, c'est l'utilisateur lui-même qui va infecter sa machine, inconsciemment évidemment, et propager le virus.

C'est typiquement le genre de virus que l'on reçoit par mail, caché à l'intérieur d'un programme en pièce jointe. En exécutant le fichier joint, l'utilisateur exécute le virus. Celui-ci infecte immédiatement la machine à la manière du TSR (reproduction + chargement en mémoire vive) et se propage automatiquement en s'envoyant lui-même par mail à tous les contacts présents dans le carnet d'adresses de l'utilisateur.

Les chevaux de Troie (Trojan Horses) ou troyens

Le cheval de Troie a pour but, comme le laisse entendre son nom, de créer une porte cachée (*backdoor*) qui permettra à son créateur d'entrer discrètement sur la machine infectée.

Le troyen est habituellement utilisé par un hacker. Ce dernier peut obtenir l'accès à une machine spécifique, comme par exemple un serveur d'une grande société dont les données présentent un intérêt. Il peut également " réquisitionner " les ressources de la machine d'un internaute afin d'y stocker des données illicites sans prendre de risques, d'envoyer des millions de spams sans pouvoir être inquiété, ou de s'en servir comme relais pour lancer une attaque sur une autre machine sans que l'on puisse remonter sa piste.
Il peut également être lancé au hasard par son créateur dans le but de créer un groupe (*pool*) de machines zombies. Dans ce cas, le troyen est programmé pour avertir son créateur de l'identité de chaque machine infectée. Toutes les machines zombies sont destinées à être utilisées pour des actions illicites ultérieurement.

2. Comment en guérir ?

Pour les virus, nous pouvons comparer la relation qu'ils entretiennent avec les ordinateurs avec celle que les hommes entretiennent avec les virus biologiques. Nous savons en guérir mais si nous ne faisons pas attention nous en attrapons.

La solution la plus efficace pour ne pas attraper de virus ou pour s'en débarrasser est l'utilisation d'un anti-virus mais cela n'empêche pas l'utilisateur de rester vigilant.

Un antivirus est un logiciel qui possède une base de données recensant les morceaux de code des virus connus *(signatures)*. Il comprend en général des composants suivants :

- *Un scanner* : programme qui permet de rechercher une éventuelle signature dans chaque fichier présent sur l'ordinateur.
- *Un gardien* : programme en mémoire qui analyse en temps réel tous les programmes manipulés par l'ordinateur. Ceux-ci peuvent être de simples applications lancées par l'utilisateur mais peuvent également se révéler être des virus tentant de se reproduire. Dans ce cas, si une signature est reconnue, le gardien alerte l'utilisateur en le prévenant qu'un virus est probablement actif sur l'ordinateur et empêche le virus de continuer son exécution.
- *Un module de mise à jour* automatique ou manuelle de la base de données de virus par connexion directe sur le site de l'éditeur du logiciel.

Le principe de fonctionnement d'un anti-virus est assez simple, il scanne ou surveille les fichiers de l'utilisateur et s'il détecte une signature de virus connu alors il peut en fonction de la stratégie adoptée par l'utilisateur :

- Désinfecter le fichier s'il le peut.
- Le mettre en quarantaine.
- Supprimer le fichier. *Attention* : cette action peut détruire des fichiers contenant des informations très importantes. Il faut donc l'utiliser avec prudence et parcimonie.

3. Prévention et prudence

Un autre moyen de lutter contre les virus est de s'intéresser aux failles qu'ils exploitent. Étant entendu que chaque nouveau logiciel ou système d'exploitation comporte fatalement des erreurs de programmation, des cas ou des schémas non recensés par les programmeurs, celles-ci sont quasiment impossibles à éviter.

Cependant, elles sont en général rapidement corrigées, la découverte d'un nouveau virus étant accompagnée de la découverte de la faille correspondante. Les éditeurs des logiciels publient donc régulièrement des mises à jour de sécurité (ou patches correctifs).
Ceux-ci se présentent généralement sous forme de programmes qui, une fois exécutés, se chargent de remplacer le code défaillant, et qui sont largement diffusés sur Internet. Afin de pouvoir s'y retrouver, les logiciels sont pourvus d'un numéro de version auquel on accède en principe grâce à une rubrique " A propos de... " dans le menu " Aide ". Il suffit alors de comparer ce numéro avec celui de la version courante du logiciel, disponible sur le site de l'éditeur pour s'assurer que le logiciel est bien à jour.
Enfin, grâce à la démocratisation d'Internet, ces mises à jours sont automatiques (on parle d'auto-update, de live-update) sur certains logiciels, et se font de manière pratiquement transparente pour l'utilisateur.
La grande rapidité avec laquelle les failles sont aujourd'hui " patchées " amène les créateurs de virus à se pencher de plus en plus vers la dernière faille, celle que les éditeurs ne peuvent pas corriger, la " faille utilisateur ". Voilà pourquoi aujourd'hui dans la majorité des cas, c'est l'internaute lui-même qui infecte sa machine. Contre cette nouvelle forme de contamination, il n'y a que deux règles à respecter : prudence et bon sens.



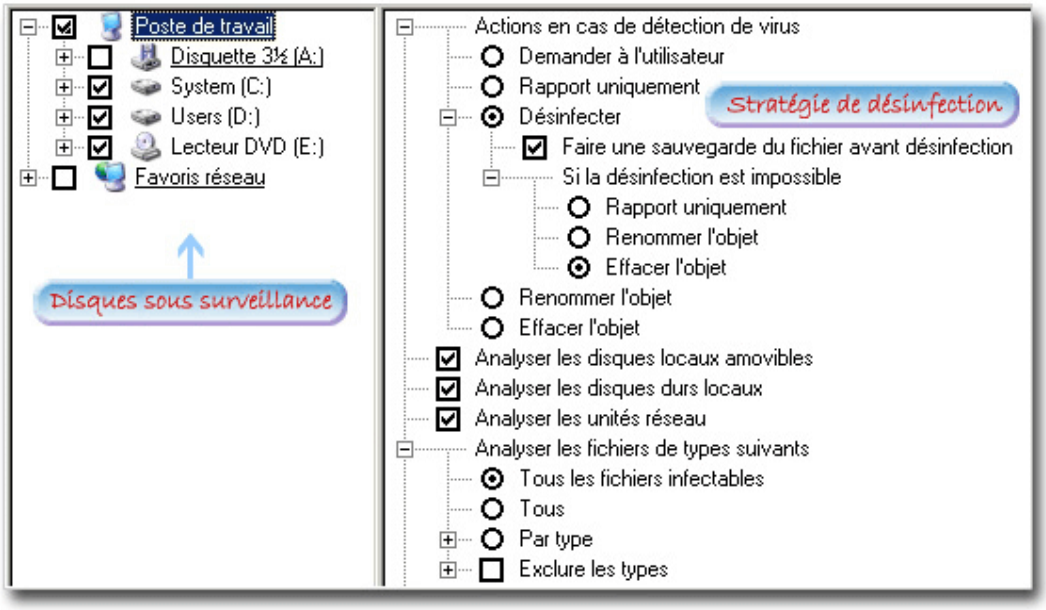
Conseil

Lors de la réception d'un e-mail contenant un fichier en pièce jointe, il est utile de se poser quelques questions : Est-ce que je connais l'expéditeur ?
Si c'est le cas, le contenu du mail lui même (langue utilisée, signature, etc.) me permet-il d'être sûr que c'est bien lui qui a rédigé ce courrier ?
Enfin, un analyse de la pièce jointe à l'aide du scanner avant de l'ouvrir n'est pas une mauvaise idée si vous possédez un anti-virus.

4. Principaux réglages d'un antivirus

Attention !

Attention



▲ IMG. 2

Dans cet exemple le lecteur de disquettes n'est pas sous surveillance ce qui fait courir un grand risque d'infection à votre machine. Faites en sorte que le moniteur surveille tous les disques fixes ou amovibles liés à votre ordinateur.

Réglage du scanner

En mode scanner seuls les disques fixes sont à analyser (dans la figure ci-dessus : C et D).

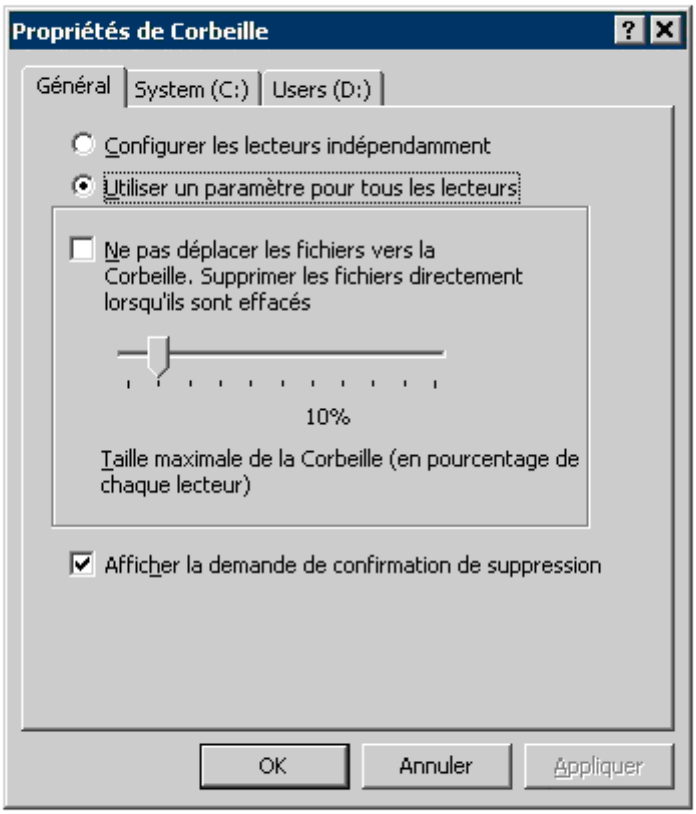
Vous pouvez garder la même stratégie de désinfection par contre il est préférable de choisir " Tous " dans la rubrique " Analyser les fichiers de types suivants ".

Partie C. Prévenir la perte de données

Pour prévenir la perte de données vous devez paramétrer correctement votre corbeille, assurer le bon état de votre machine et assurer des sauvegardes régulières.

1. Paramétrer correctement sa corbeille

Dans la partie précédente nous avons vu comment se protéger des virus. Mais l'utilisateur peut de lui même provoquer la perte de données par un effacement accidentel. Pour éviter cela, ne jamais désactiver la corbeille. En effet, cette dernière stocke tous les fichiers effacés par l'utilisateur. Ainsi, un fichier effacé accidentellement peut être facilement récupéré. Les fichiers contenus dans la corbeille seront définitivement perdus lorsque l'utilisateur videra la corbeille.



▲ IMG. 3 : PARAMÉTRAGE DE LA CORBEILLE SOUS WINDOWS XP

Remarque
Rien n'est jamais définitif ! Si vous vous apercevez que vous avez vidé votre corbeille alors que vous aviez accidentellement jeté un fichier vous avez encore une chance de le récupérer à l'aide d'un logiciel spécifique.

2. Surveiller le bon état de votre machine

Tous les accidents ne sont pas prévisibles mais l'utilisateur peut agir de manière à éviter certains désagréments.

L'installation d'un onduleur évitera lors d'une coupure de courant la perte des données en cours d'utilisation. Il n'est pas uniquement destiné à pallier les coupures de courant, son rôle est également de stabiliser la tension électrique et d'éliminer les parasites qui sont des causes éventuelles de pannes matérielles.
L'arrêt de la machine ou la mise en veille lorsque l'on ne l'utilise pas, évitera une fatigue prématurée des disques durs et abaissera le risque de panne surtout lors des fortes chaleurs.

3. Assurer une sauvegarde



Remarque
La meilleure façon de prévenir la perte de données est d'assurer une sauvegarde régulière de vos données personnelles.
Voir chapitre " Assurer une sauvegarde (sur le réseau, support externe, ...) "

Partie D. Exercices - QCM

Exercice n°1. Assurer la protection de sa machine

Sésame, ouvre-toi !

Enoncé : Faites une analyse de la situation de vos différents mots de passe (élargissez éventuellement votre réflexion avec les numéros de CB, compte, ...) et après la réflexion, améliorez tout cela.

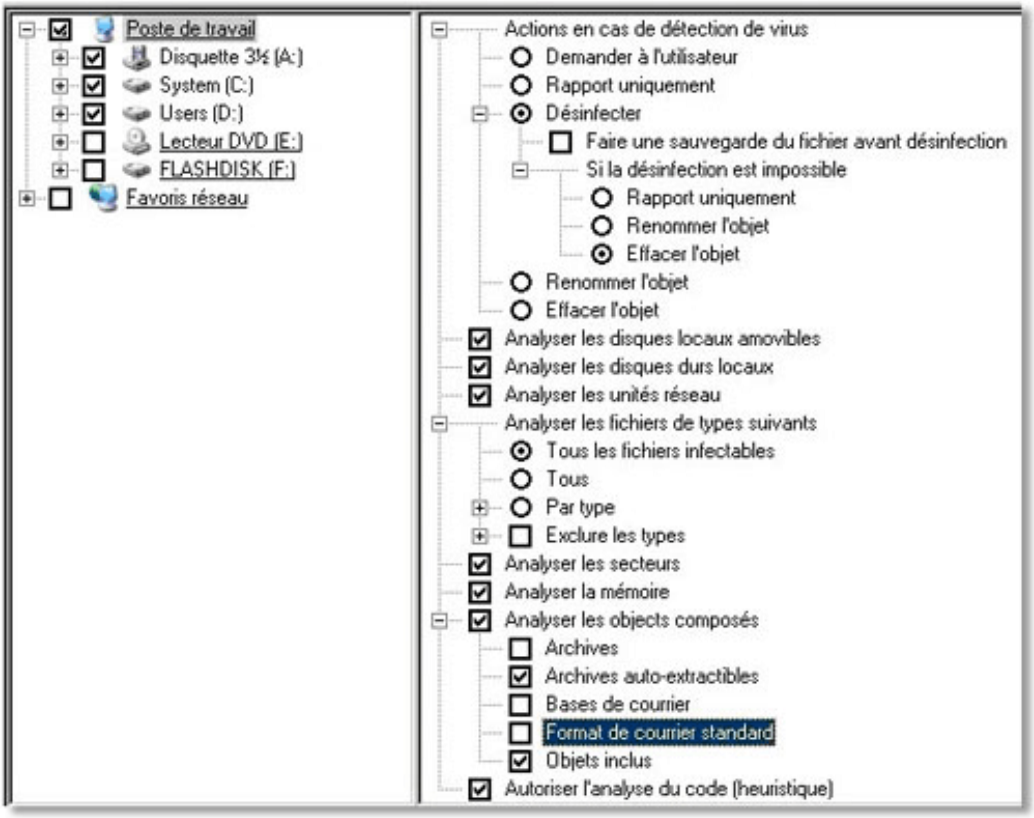
- Sont-ils tous différents ?
- Combien sont connus de quelqu'un d'autre ou notés quelque part ?
- Quelle est leur longueur ?
- Sont-ils en rapport avec vos données personnelles ?

Recyclage ?
Enoncé : Allez-voir quelle est la configuration de votre corbeille.

Exercice n°2. Assurer la protection contre les virus

Sus à l'ennemi !!!

Enoncé : Ceci est une capture d'écran du réglage d'un gardien, tel qu'il vous a été présenté dans le cours.



▲ IMG. 4

- Quels sont les périphériques qui seront vérifiés par le gardien ?
- Identifiez si le gardien est en mode automatique ou en mode manuel.
- Quelle est l'action qui sera faite par le gardien en cas de détection de virus ?
- Critiquez cette configuration.
- Proposez une autre configuration.

Prudence...

Enoncé : Voici le mail que vous venez de recevoir. Que faîtes-vous ?

X-Sieve: CMU Sieve 2.2

Date: Thu, 30 Jun 2005 18:47:28 +0200
From: camara abu camaraabu@go.com
User-Agent: Mozilla Thunderbird 1.0.2 (Windows/20050317)
X-Accept-Language: fr, en T
o: moi moi@caramail.com
Subject: b4
X-Bogosity: No, tests=bogofilter, spamicity=0.000000, version=0.94.12

Voici le fichier ;-)

X-PREPEND-UT1: suscpicious_attachement
X-PREPEND-UT1: suscpicious_attachement
Content-Type: unknown
name=" C45ezw34.exe"
X-PREPEND-UT1: suscpicious_attachement
X-PREPEND-UT1: suscpicious_attachement
Content-Disposition: inline;
filename=" C45ezw34.exe"

Alerte !!!

Enoncé : Voici le mail que vous venez de recevoir. Que faîtes-vous ?

X-Sieve: CMU Sieve 2.2
Date: Thu, 30 Jun 2005 18:47:28 +0200
From: toto@univ_bid1.fr
User-Agent: Mozilla Thunderbird 1.0.2 (Windows/20050317)
X-Accept-Language: fr, en
To: moi moi@caramail.com
Subject: Attention, nouveau virus
X-Bogosity: No, tests=bogofilter, spamicity=0.000000, version=0.94.12
Attention, un nouveau virus a été récemment découvert par l'institut Norton Anti-Virus. Il se présente sous la forme d'un fichier nommé excel.exe et se trouve généralement dans le répertoire C:\PROGRAM FILES\APPLICATIONS\OFFICE\EXCEL. Celui-ci étant très dangereux, veillez à le détruire le plus rapidement possible.
Votre dévoué,

Exercice n°3. Assurer la protection de sa machine - Questions



Question1
Comment définiriez-vous un "bon" mot de passe ?



Question2
Qu'est-ce qu'un firewall ?



Question3
Quelles sont les différentes politiques de sécurité d'un firewall ?

Exercice n°4. Assurer la protection contre les virus - Questions

Question1
Quels sont les trois types de virus que l'on peut trouver ?

Question2
Comment se propagent les virus ?

Question3
Existe-t-il des virus inoffensifs ?

Question4
Quels moyens avez-vous de vous protéger des virus ?

Question5
Un virus informatique est :
- un programme
- une maladie
- un courrier indésirable
- je ne sais pas

Question6
Un ver informatique est :
- un animal sans pattes
- un virus qui se propage de façon autonome au travers du réseau
- une machine zombie qui sert de support à des opérations illicites
- je ne sais pas

Question7
Certains virus permettent de créer des points d'accès sur différentes machines. Ce sont :
- des virus d'application
- des virus réseaux
- des troyens
- je ne sais pas

Question8

Je peux me protéger des virus en utilisant :

- un anti-virus à jour
- un firewall
- une adresse mail inconnue
- un mot de passe très compliqué

Question9

Un anti-virus comporte :

- un gardien
- un espion
- un détecteur
- je ne sais pas

Question10

Un scanner est :

- une machine à numériser les virus
- un logiciel qui permet de rechercher les virus
- un détecteur de problèmes de vos disques durs
- je ne sais pas

Chapitre

II

Se protéger de la malveillance

Objectifs pédagogiques

Comme la perte de données, la malveillance peut être le fait d'un autre utilisateur mais aussi d'un logiciel qui s'invite sur votre ordinateur afin de vous espionner.

Lecture ou copie de fichiers privés, lecture de votre courrier électronique, suivi de votre navigation sur Internet, lecture d'informations de votre environnement de travail, modification du contenu d'un fichier sont des exemples d'actions malveillantes même s'il n'y a pas forcément envie de nuire.

Le but de ce chapitre est que l'apprenant puisse :

- Identifier et évaluer les risques de malveillance de son environnement.
- Savoir se protéger de la malveillance.
- Agir de manière préventive.



Démarche

Nous allons dans un premier temps découvrir comment se protéger des mouchards puis nous verrons les précautions à prendre afin de se prémunir de la malveillance. La dernière partie explicite notamment le but et les principes de la cryptographie.

Partie A. Assurer la protection contre des mouchards (spyware)

Les spywares

Bien qu'à première vue anodin, le marché de la publicité sur Internet représente des sommes colossales qui expliquent cet acharnement à proposer aux annonceurs des services adaptés. La fin justifiant les moyens, les sociétés éditrices de spywares n'hésitent pas à sacrifier la vie privée et la confidentialité des données des internautes sur l'autel du profit.



Spyware
Les spywares ont pour but l'espionnage des habitudes de l'internaute dans le but de pouvoir cibler la publicité qui lui est proposée sur le web.

Le spyware a pour but de récolter un maximum d'informations sur l'utilisateur (les logiciels installés sur sa machine aussi bien que ses habitudes sur le web telles que les sites qu'il consulte, les publicités qui l'intéressent, etc.) et les envoyer vers un serveur où elles seront compilées et traitées.

Le spyware se charge en mémoire vive au démarrage de la machine et rapporte les moindres faits et gestes de l'internaute à son centre, de manière totalement invisible pour l'internaute.

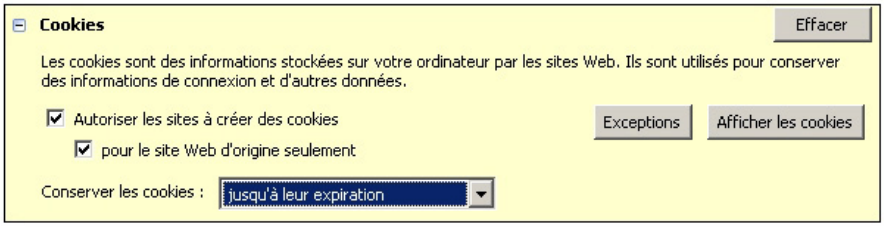
Il existe plusieurs manières de se faire infecter par un spyware :
- il peut exploiter une faille du navigateur Internet,
- être installé par un ver,
- se présenter sous la forme de petits programmes distribués en tant que modules annexes (les éditeurs préfèrent le terme de programmes partenaires) d'applications proposées gratuitement (freewares ou sharewares). Ils sont légaux car spécifiés dans les termes de la licence du programme qu'ils accompagnent.

1. Les différents types de spywares

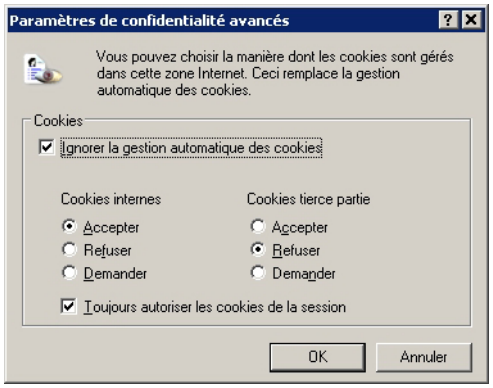
Les BHO (Browser Helper Objects) se font passer pour des modules additionnels de l'explorateur Internet (barre de recherche, filtre anti-popup, etc.). Ils remplissent les mêmes fonctions que les spywares traditionnels.

Les hijackers basés également sur le parasitage de l'explorateur Internet, remplacent la page de démarrage par la page d'une société cliente et interceptent les requêtes de l'utilisateur afin de mettre en avant les sites des sociétés clientes. Ceux-ci ne sont pas installables par l'utilisateur mais utilisent des failles du navigateur (exécution de scripts).
Une autre technique utilisée pour récolter des informations est le cookie. Celui-ci est un fichier créé et entretenu par un site web lors de la visite d'un internaute. Localisé

sur la machine de l'utilisateur, il a pour but de récolter des informations relatives au passage de l'internaute sur le site (nom, prénom, pages consultées, articles préférés, etc.), dans le but de rendre plus conviviales ses visites ultérieures. Il n'est en général pas dangereux car il est limité dans le temps, n'a pas accès aux ressources et aux données de l'utilisateur et ne peut être exploité que par le site qui l'a créé. Il ne pose de problème que dans le cas où l'ordinateur est utilisé par plusieurs personnes car chacune a accès aux informations laissées par les autres.
Les navigateurs permettent de définir des politiques de gestion des cookies : l'internaute peut refuser l'écriture de tout cookie, effacer tous les cookies dès la fermeture du navigateur, ou encore être consulté à chaque demande de création d'un cookie.



▲ IMG. 5 : RÉGLAGES DE LA GESTION DES COOKIES SOUS FIREFOX 1.0.4 (OUTILS/OPTIONS/VIE PRIVÉE/COOKIES)



▲ IMG. 6 : RÉGLAGES DE LA GESTION DES COOKIES SOUS IE 6 (OUTILS/OPTIONS INTERNET/CONFIDENTIALITÉ/AVANCÉ)

2. Lutter contre les spywares

Pour éviter d'être contaminé, certaines règles s'imposent. Lors de l'installation d'un logiciel, à plus forte raison si celui-ci est gratuit, lisez la licence attentivement (même si celle-ci est intentionnellement longue et rédigée en anglais) afin de vérifier qu'aucun " logiciel partenaire " ne soit installé contre votre gré. Lorsque vous visitez une page web et qu'on vous propose d'installer un logiciel soi-disant indispensable pour poursuivre ou un plugin, vérifiez bien l'identité de la société éditrice et refusez l'installation si vous avez le moindre doute.

Malgré ces précautions, il est hélas possible que vous soyez infecté un jour. Pour éradiquer les spywares, des logiciels appelés anti-spyware les recensent et les éliminent.
On peut citer, parmi les plus connus, les freewares :

- **Spybot-Search-and-Destroy**

  http://www.safer-networking.org/fr/home/index.html

- **Ad-Aware**

  http://www.lavasoftusa.com/



Attention
Certains anti-spywares peuvent contenir des spywares !

Partie B. Prévenir la malveillance

Se protéger de la malveillance

Pour se protéger de la malveillance deux solutions rendent difficiles l'accès à un fichier contenant des données confidentielles : les mots de passe liés au fichier ou le cryptage de fichier.

Avant cela nous allons voir deux actions qu'un propriétaire d'un fichier peut effectuer par précaution mais ces actions ne sont pas d'un grande efficacité face à un utilisateur averti.



Propriétaire d'un fichier
La notion de propriétaire est différente de la notion de créateur. Le propriétaire est la personne qui possède le fichier et non celui qui la créé.

Pour le propriétaire, la stratégie de protection est directement liée au système d'exploitation.

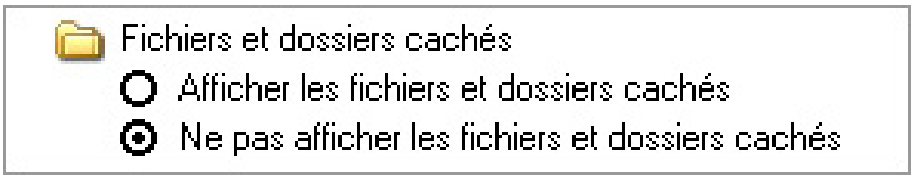
1. Protéger un fichier

En fonction des différents systèmes d'exploitation, il y a plusieurs manières de protéger un fichier.

Rendre un fichier invisible

Un fichier invisible, on parle également de fichier caché, est un fichier qui ne sera pas visible dans votre gestionnaire de fichiers.

Attention
Pour que cette action soit efficace il faut que l'option " Ne pas afficher les fichiers cachés " de votre système soit activée.



▲ IMG. 7 : OPTION DU GESTIONNAIRE DE FICHIERS DE WINDOWS XP (OUTILS/OPTIONS DES DOSSIERS/AFFICHAGE)

Mettre un fichier en lecture seule

La restriction en lecture seule interdit l'écriture. Vous évitez ainsi une modification malencontreuse.



▲ IMG. 8 : ATTRIBUTS DE FICHIER SOUS WINDOWS XP (PROPRIÉTÉS DANS LE MENU CONTEXTUEL)

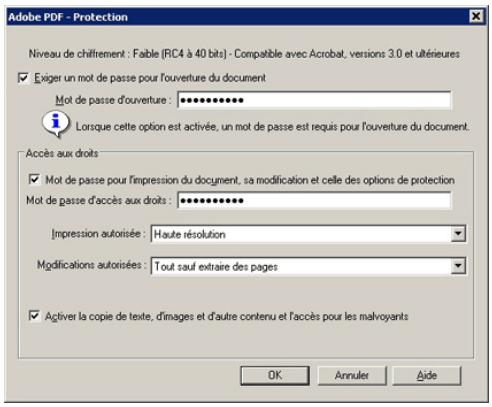
Attacher un mot de passe à un fichier

La seule manière efficace de s'assurer qu'une action malveillante ne sera pas effectuée sur votre fichier est de lui affecter un mot de passe. Cela ne peut se faire que si l'application qui vous a servi à créer le fichier offre cette possibilité.

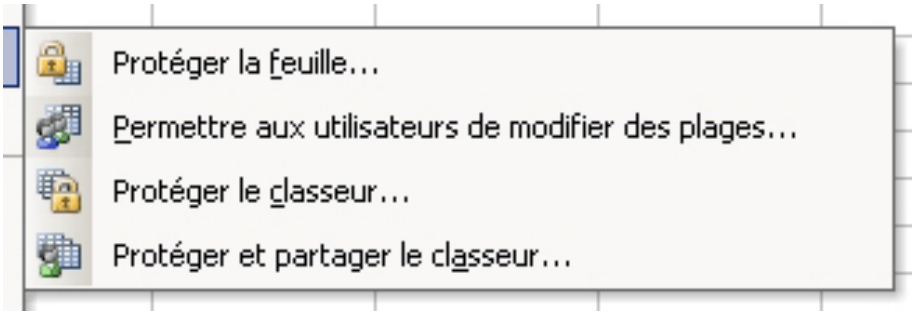
Auteur d'un fichier
L'auteur ou le créateur est celui qui a écrit le fichier. Celui-ci peut le distribuer et les personnes qui le reçoivent en deviennent alors propriétaires.
Pour le créateur, le système de protection est lié au logiciel capable de créer le fichier (indépendamment du SE). Ainsi le créateur va pouvoir limiter les actions réalisables sur son fichier en lui associant un mot de passe.

Exemple
Vous remarquerez ci-dessous que le logiciel Adobe Distiller 6 permet d'associer un mot de passe à l'ouverture du fichier mais également à l'impression et à la modification.

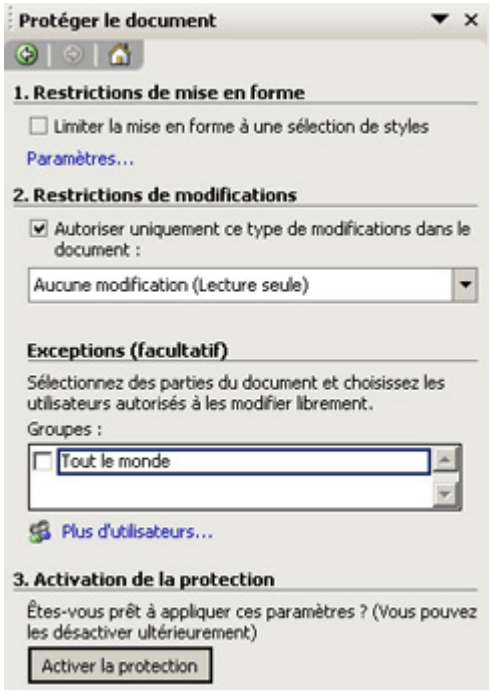
Un autre exemple sera vu dans le chapitre " Compresser/décompresser ses données ", en effet lors de la création d'archive nous pouvons poser un mot de passe sur un fichier ajouté afin d'empêcher sa décompression par des personnes non autorisées.



▲ IMG. 9 : PROTECTION SOUS ADOBE DISTILLER 6



▲ IMG. 10 : OPTIONS DE PROTECTION PROPOSÉES PAR EXCEL 2003 (OUTILS/PROTECTION)



▲ IMG. 11 : OPTIONS SOUS WORD 2003 (OUTILS/PROTÉGER LE DOCUMENT)

2. Crypter un fichier

Pour communiquer l'homme a toujours ressenti le besoin de dissimuler des informations bien avant même l'apparition des premiers ordinateurs et de machines à calculer. Le but est d'éviter qu'une personne parvenant à intercepter le message ne puisse le lire. Pour cela les deux correspondants s'inventent un autre langage de communication et des procédures de chiffrement et de déchiffrement du message.



Cryptographie
Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffrer.

Aujourd'hui la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

- La *confidentialité* consiste à rendre l'information inintelligible à d'autres personnes que les acteurs de la transaction.
- Vérifier *l'intégrité des données* consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- *L'authentification* consiste à assurer l'identité d'un utilisateur, c'est-à-dire à garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

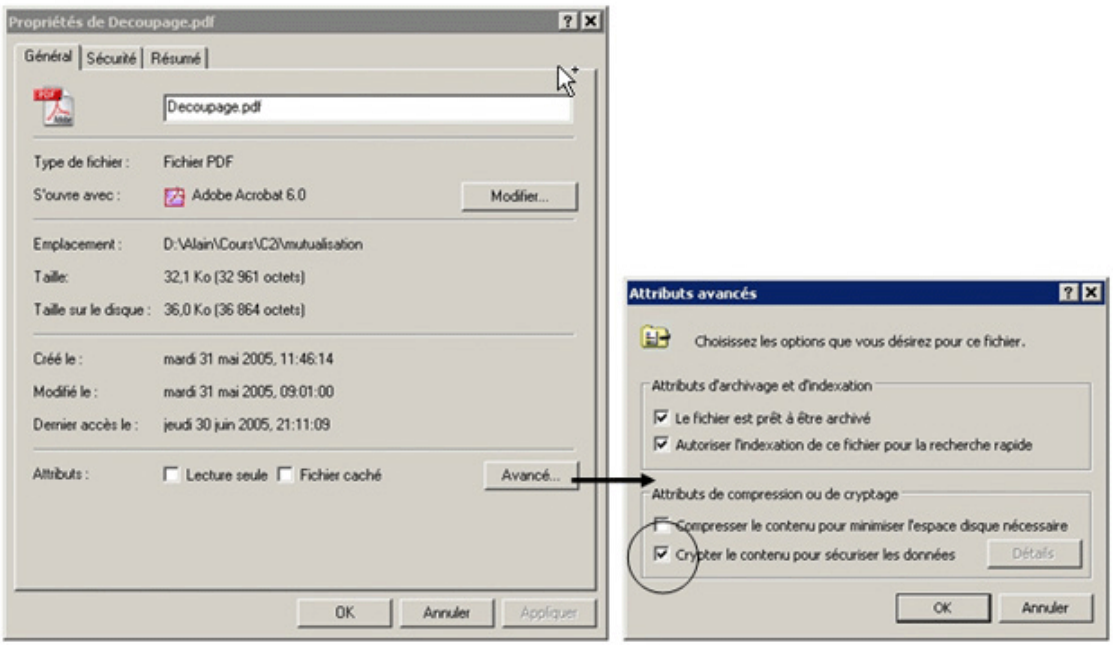
Crypter des données sous Windows XP Pro

Windows XP utilise le système EFS (Encrypting File System) pour enregistrer des fichiers dans un format crypté sur votre disque dur. Les fichiers cryptés seront impossible à lire par les autres utilisateurs de votre machine mais notez que les administrateurs peuvent déchiffrer les données qui ont été cryptées par un autre utilisateur.

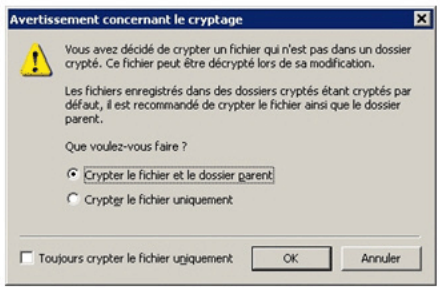
Vous pouvez crypter des fichiers uniquement sur des volumes NTFS (système de fichiers NT). Pour crypter un fichier, procédez comme suit :

1. Cliquez sur Démarrer, pointez sur Programmes, sur Accessoires, puis cliquez sur Explorateur Windows.
2. Recherchez le fichier souhaité, cliquez sur celui-ci avec le bouton droit, puis cliquez sur Propriétés.
3. Dans l'onglet Général, cliquez sur Options avancées.
4. Sous Attributs de compression ou de cryptage, activez la case à cocher Crypter le contenu pour sécuriser les données, puis cliquez sur OK.
5. Cliquez sur OK. Si le fichier se situe dans un répertoire non crypté, la boîte de dialogue Avertissement concernant le cryptage s'affiche. Suivez l'une des étapes ci-après :

- Si vous souhaitez crypter uniquement le fichier, cliquez sur Crypter le fichier uniquement, puis cliquez sur OK.
- Si vous souhaitez crypter le fichier et le répertoire dans lequel il se trouve, cliquez sur Crypter le fichier et le dossier parent, puis cliquez sur OK.



▲ IMG. 12



▲ IMG. 13 : CRYPTAGE SOUS WINDOWS XP PRO

Les fichiers cryptés ne peuvent pas être ouverts, copiés ou déplacés par d'autres utilisateurs. Par exemple, si un autre utilisateur tente d'ouvrir un fichier Microsoft Word crypté, il reçoit un message de type : " Impossible d'ouvrir le fichier : nom_de_l'utilisateur ne possède pas les droits d'accès ".

Cryptage sur Internet

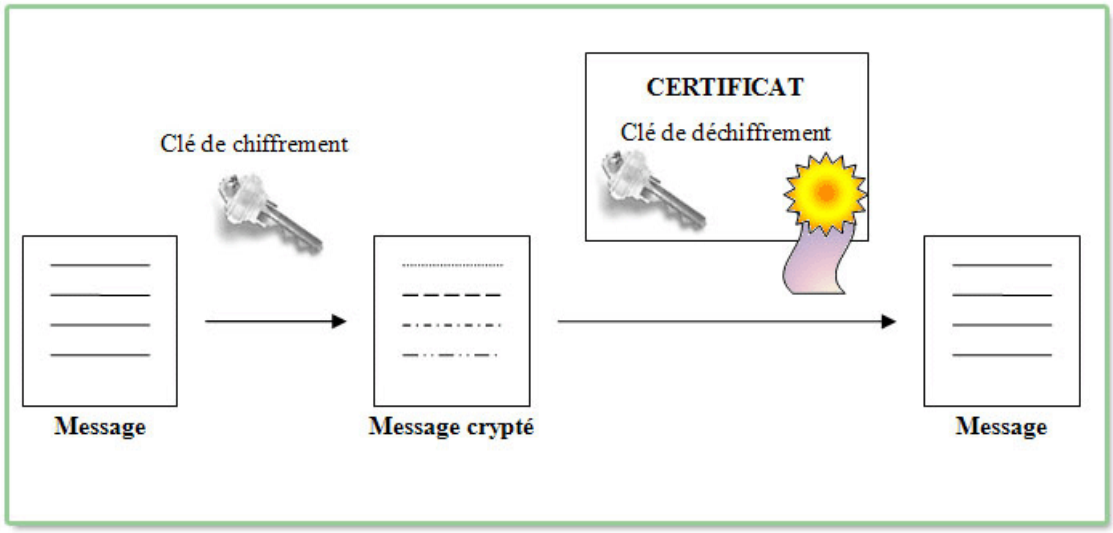
La signature numérique

Actuellement le type de cryptage le plus utilisé est un *chiffrement asymétrique* avec une clé de chiffrement et une clé de déchiffrement différentes. Découvrons cela à

travers la signature numérique.
Quand vous signez un papier, vous apposez une marque personnelle. Cette dernière rend le fichier unique et identifie le créateur. En numérique, plus de stylo, la marque d'un utilisateur est une clé de chiffrement.
Dès lors, *signer un fichier* signifie chiffrer le fichier avec votre clé de chiffrement. Donc pour déchiffrer le fichier il faudra posséder une clé de déchiffrement qui permettra de retrouver le message d'origine.
Ces deux clés forment un tout car la clé de déchiffrement ne peut déchiffrer que les messages chiffrés par la clé de chiffrement associée.
La clé de chiffrement (*clé privée*), qui est unique car elle permet de vous identifier, doit rester secrète et ne doit pas être distribuée pour éviter qu'une personne ne chiffre à votre place. Donc pour permettre aux autres de lire vos fichiers vous allez leur donner votre clé de déchiffrement (*clé publique*).

Les avantages de la signature numérique à l'aide d'un chiffrement asymétrique sont les suivants :

- La signature numérique n'est pas imitable. Il est impossible d'imiter votre signature numérique et personne ne pourra signer un fichier à votre place s'il ne possède pas votre clé privée car votre clé publique ne pourra pas déchiffrer le fichier (dans le monde papier il suffit de faire une photocopie).
- La signature numérique n'est pas répudiable. La non répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier une transaction. Par exemple : si une personne vous fait une reconnaissance de dette manuscrite sans passer devant notaire, elle peut au moment où vous réclamez votre argent, prétendre que vous avez imité sa signature. Avec la signature numérique cela est impossible car le signataire aura utilisé sa clé privée qu'il est le seul à connaître !
- La signature numérique protège le contenu contre les modifications. Après la signature d'un rapport de plusieurs pages, si une des pages est modifiée à votre insu alors vous ne pouvez rien prouver. Or un fichier signé numériquement dépend de son contenu donc si le contenu change le fichier signé changera et ne sera donc plus identique au premier fichier signé.
- La signature numérique permet de signer les oeuvres numériques multimédias (musiques, photos, ...) ce qui identifie le créateur.



▲ IMG. 14 : LE PRINCIPE DE LA SIGNATURE NUMÉRIQUE

Les certificats d'authenticité

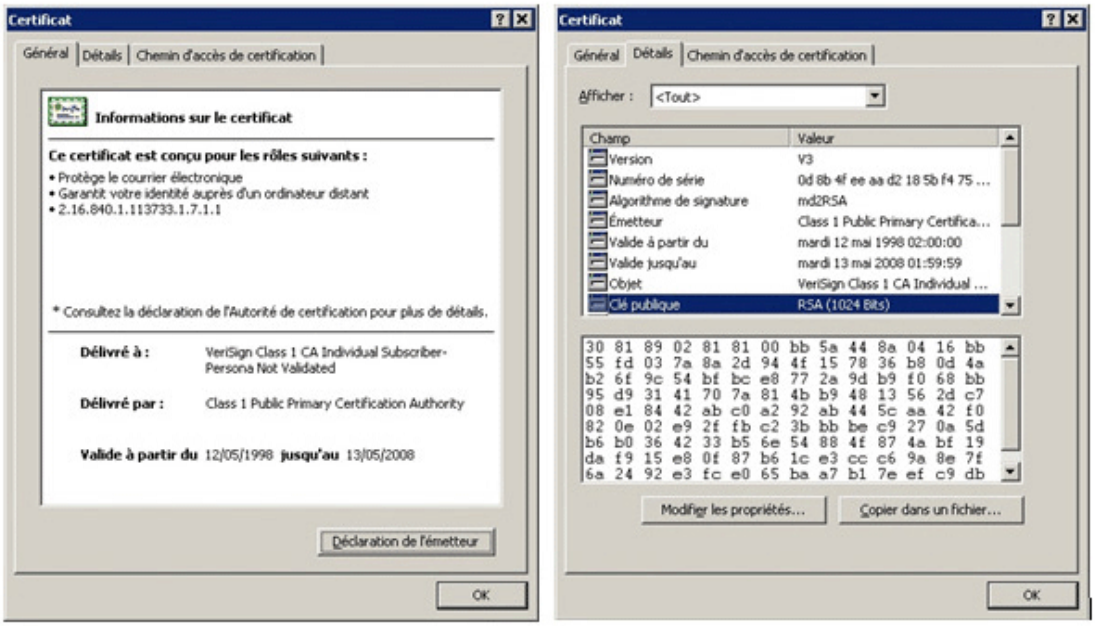
Attention
Un message chiffré ne signifie pas que le message n'est pas malveillant. En effet, une personne peut très bien chiffrer un virus.

Lorsque vous signez un chèque, on vous demande une pièce d'identité ce qui permet de comparer la signature sur la pièce et la signature apposée.

Ce même principe est utilisé pour les signatures numériques. Afin d'autoriser une personne à déchiffrer votre signature vous lui fournirez un certificat qui contiendra notamment votre clé publique, votre identité, l'identité de l'organisme certificateur et la date de validité de votre certificat.

Exemple : Gestion des certificats sous IE 6.
Pour voir les différents certificats enregistrés sur votre machine par IE 6, faites " Outils/Options Internet " puis dans l'onglet " Contenu " cliquez sur " Certificats ".

Les boîtes de dialogue ci-dessous montrent les informations générales sur le certificat et notamment la clé publique, l'identité de l'émetteur, l'identité de l'organisme certificateur et la date de validité du certificat.



▲ IMG. 15

Le système est-il fiable ?

Oui mais il ne résistera jamais au temps !

Comme un mot de passe, on peut retrouver une clé en essayant toutes les combinaisons possibles mais le temps de calcul est tellement long que le système peut être considéré comme fiable.
L'algorithme à clé publique le plus utilisé actuellement est *RSA* (Rivest, Shamir, et Adelman). Récemment un projet " vachement ambitieux " nommé RC5 Bovine invite n'importe quel internaute du monde entier à rechercher une clé publique. L'internaute télécharge un programme qui fonctionne en autonomie. Ce dernier utilise la puissance de calcul de l'ordinateur de l'internaute pour casser la clé et se connecte régulièrement à un serveur central qui lui envoie la liste des codes suivants à tester. L'addition de tous les internautes participant au projet offre une puissance de calcul gigantesque.
La clé de 56 bits a été trouvé en 256 jours, la clé de 64 bits a été trouvé en 1757 ; aujourd'hui, 29 juin 2005, le projet tente de casser une clé de 72 bits, nous sommes au 939ème jour de calcul.



Remarque sur la législation

Il existe des lois sur Internet, cependant elles sont souvent inadéquates et chaque pays a sa propre législation, si bien que la France interdisait il y a encore quelques années tout chiffrage (excepté la signature depuis 1990) car les politiciens considéraient (certains encore aujourd'hui) que le citoyen ne devrait pas avoir accès à des moyens cryptographiques pouvant servir aux militaires. La politique française s'est assouplie depuis mais reste encore en marge par rapport à des pays comme les Etats-Unis qui laissent la liberté à leurs citoyens de crypter à loisir.

La nouvelle législation française autorise n'importe quelle personne (physique ou morale) à utiliser un logiciel de chiffrement à condition de déposer les clés auprès d'un organisme agréé par la DCSSI (Direction Centrale de Sécurité des Systèmes d'Information). Celui-ci pourra remettre les clés de chiffrement à la justice en cas de doute. Ce Tiers de confiance ne dépend pas de l'Etat, ce dernier doit mettre en place une procédure judiciaire pour pouvoir contrôler des messages chiffrés.

Partie C. Exercices - QCM

Exercice n°5. Associer un mot de passe à un document (Windows, Excel)

Enoncé :

1. Ouvrez Excel
2. Créez un nouveau classeur nommé motpasse.xls sous le dossier Mes Documents
3. Associez un mot de passe à ce classeur (menu Outils/Protection)
4. Fermez Excel
5. Placez-vous dans le dossier Mes Documents. Double-cliquez sur le classeur motpasse.xls
6. Rendez ce document invisible

Exercice n°6. Questions



Question1

Qu'est-ce qu'un mouchard ?

Donnez un autre terme pouvant désigner un mouchard.



Question2

Quel mode de propagation peut utiliser un mouchard ?

Question3
En quoi le cookie est-il utile aux spywares ?

Question4
Qu'est-ce que la confidentialité ?

Question5
Qu'est-ce que l'intégrité des données ?

Question6
Qu'est-ce que l'authentification ?

Question7
La signature numérique est-elle fiable ?
Etayez votre réponse.

Question8
Je reçois un message dont le fichier joint est crypté.
- je peux donc l'ouvrir sans souci d'être infecté par un virus.
- je dois toujours me méfier et utiliser mon anti-virus
- je ne sais pas quoi faire

Question9
La signature numérique d'un document consiste :
- A y associer un code convenu avec votre correspondant
- A y associer votre signature scannée
- A y associer une clé de chiffrement
- Je ne sais pas

Question10
Un certificat d'authenticité permet :
- de dater de façon certaine le document
- de déchiffrer le document
- d'identifier parfaitement l'envoyeur
- Je ne sais pas



Question11

Pour signer un document destiné à une autre personne, j'utilise :

- ma clé privée
- ma clé publique
- n'importe laquelle, les deux m'appartiennent



Question12

Pour déchiffrer un document signé il faut posséder :

- la clé publique
- la clé privée
- les deux
- cela dépend du contenu

Chapitre

III

Se préserver des nuisances

Objectifs pédagogiques

Ce chapitre est réservé aux nuisances induites par le développement de l'informatique et d'Internet. De nouvelles formes de nuisances viennent tous les jours importuner les utilisateurs.

Le but de ce chapitre est de découvrir quelles sont ces nuisances et surtout comment s'en préserver.

Nous ne parlerons que des pourriels (spam) et des canular (hoax) mais nous pouvons classer comme nuisances :

- Les pop-ups : ces fenêtres publicitaires qui jaillissent pendant la navigation.
- Les jeux concours similaires à ce que l'on reçoit dans nos boîtes aux lettes.

Partie A. Les pourriels ou spams

Définition des pourriels

Actuellement le phénomène reconnu comme le plus envahissant est le pourriel (spam).



Pourriels (ou spams)
Courriers électroniques non sollicités ou indésirables, les spams ne présentent pas réellement de danger mais sont une nuisance qui prend plus d'ampleur chaque jour.

Ce terme englobe tout courrier envoyé à un utilisateur sans son consentement (on parle

d'opt-in). Dans la majorité des cas, il a un but publicitaire ou promotionnel.

La LEN (la Loi sur l'Economie Numérique) ayant défini un cadre strict en ce qui concerne la publicité par voie électronique, la prospection est autorisée en France " si les coordonnées du destinataire ont été recueillies directement auprès de lui, à l'occasion d'une vente ou d'une prestation de services, et concernant des produits ou des services analogues à ceux visés par la prospection " (source : leJournalduNet). Le spam concerne donc tous les autres courriers publicitaires ou promotionnels, en général pour des sites étrangers de vente de produits pharmaceutiques, des sites pornographiques, etc. Il est envoyé en masse et surtout illégalement à partir de machines " zombies " ou de comptes mails piratés.

Le but pour l'annonceur est de pouvoir toucher le plus de monde, ce qui implique de posséder un nombre important d'adresses mail valides. Des fichiers recensant des millions d'adresses mail se vendent ou se louent à prix d'or. Les moyens de collecte de toutes ces adresses mails sont nombreuses :

- Les spammeurs utilisent des " robots " qui scannent les pages web et recensent toutes les adresses qu'ils y trouvent.
- Une autre méthode consiste à envoyer du courrier à l'aveugle, c'est-à-dire en générant des adresses électroniques aléatoires, puis vérifier celles qui sont valides.

  Comment ? Ces courriers ne font pas de publicité mais vous annoncent que vous avez gagné un voyage, un appareil électronique très coûteux ou un lot quelconque. Etant donné qu'ils sont envoyés à des adresses de messagerie générées aléatoirement, ils s'adressent à vous en vous appelant par votre login de messagerie ! Evidemment, le lot promis ne vous sera jamais remis !

  Le but de ce genre de courrier est de vous faire cliquer sur un lien qui avertira le spammeur que vous avez bien reçu le mail et que par conséquent votre adresse de messagerie est valide. Celle-ci sera immédiatement enregistrée dans un fichier pour être vendue.

1. Lutter contre le spam

Pour lutter contre le spam, il faut d'abord en cerner le fonctionnement. Votre adresse de messagerie n'est pas a priori publique et n'est pas référencée dans un annuaire. Afin de conserver cette confidentialité :

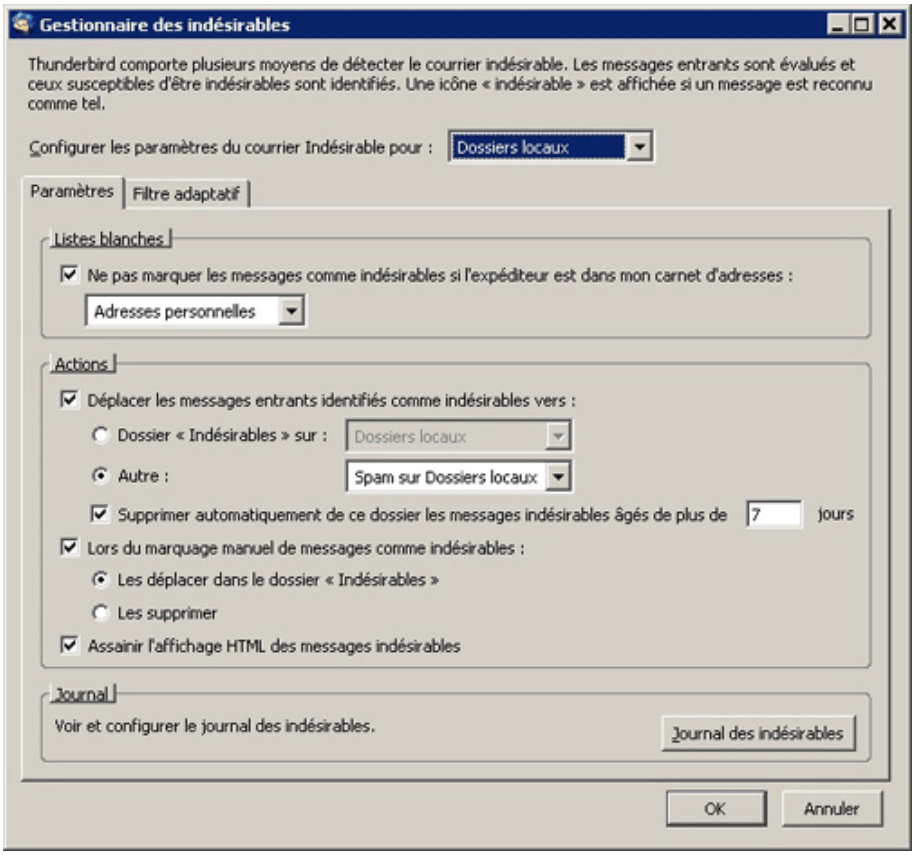
- Ne la communiquez jamais quand on vous la demande sur un site web, à moins d'être sûr que ce site ne l'exploitera pas illégalement ! Si le site vous impose de donner une adresse valide, pour avoir accès à une zone restreinte par exemple, sachez que vous pouvez toujours créer une adresse temporaire sur le site KasMail.com ou une adresse "poubelle" gratuite sur hotmail, caramail, yahoo, etc.
- Évitez de laisser votre adresse dans les forums, les groupes de discussion ou sur votre site web. Masquez-la (par exemple : remplacer " nom@domaine.fr " par " nom chez domaine point fr " ou encore " PASnomDE@domaineSPAM.fr ") ou bien là encore, utilisez une adresse poubelle. Autre possibilité : insérez-la sous forme d'image, les robots seront incapables de la détecter.
- Enfin et surtout, ne répondez JAMAIS à un spam ! Ne cliquez sur aucun lien du mail, même si on vous assure qu'il sert à vous désinscrire de la liste de diffusion ! Si vous cliquez, au lieu de résoudre le problème vous l'amplifiez !

De plus en plus, les fournisseurs d'accès proposent un service permettant de stopper les spams que vous recevez. Pour cela ils installent un anti-spam qui filtre les messages supposés indésirables.

Si votre fournisseur d'accès ne vous offre pas cette possibilité, optez pour une messagerie intégrant un anti-spam. La messagerie gratuite *Mozilla Thunderbird* permet d'effectuer le filtrage des courriers indésirables. Pour cela vous allez pendant quelques jours entraîner votre filtre anti-spam en lui désignant effectivement quels sont les courriers indésirables. Le filtre analyse les courriers désignés et recherche une caractéristique essentielle qui lui permettra de le reconnaître ultérieurement comme spam.
On retrouve ici le principe de la signature des virus à la différence que l'anti-spam se crée sa propre " image " de la signature du spam ce qui le rend adaptatif. Il y a tout de même un petit inconvénient, il est possible qu'un courrier désirable soit pris pour spam car il est proche de la signature imaginée par le filtre. Pour éviter ce petit ennui *Mozilla Thunderbird* propose de reclasser le courrier comme désirable ce qui oblige le filtre à modifier sa mauvaise signature. Il propose également une liste blanche c'est-à-dire une liste de personnes considérées comme sûres dont les mails ne seront pas filtrés.



Conseil
Essayez Mozilla Thunderbird, vous l'adopterez !



▲ IMG. 16 : GESTION DES INDÉSIRABLES DE MOZILLA THUNDERBIRD



Démarche

Et si mon filtre devient fou et se met à classer tous mes messages comme indésirables ! Ne vous inquiétez pas vous pouvez " remettre à zéro " votre filtre et lui réapprendre à filtrer.

2. Arnaques et escroqueries

Le scam et le phishing représentent les formes de spam les plus dangeureuses puisqu'elles ont pour unique but, avec abus de confiance, d'extorquer de l'argent à un internaute.

Le scam

Un scam est généralement envoyé par un millionnaire étranger qui possède une fortune bloquée en France. Le hasard a fait que vous êtes en mesure de l'aider à récupérer cette somme colossale. Vous êtes son seul espoir ! Evidement, pour le coup de main, vous toucherez un pourcentage dès que la somme sera débloquée, c'est-à-dire dès que vous aurez accepté d'avancer certains frais d'avocats, de douanes, etc.

Le phishing

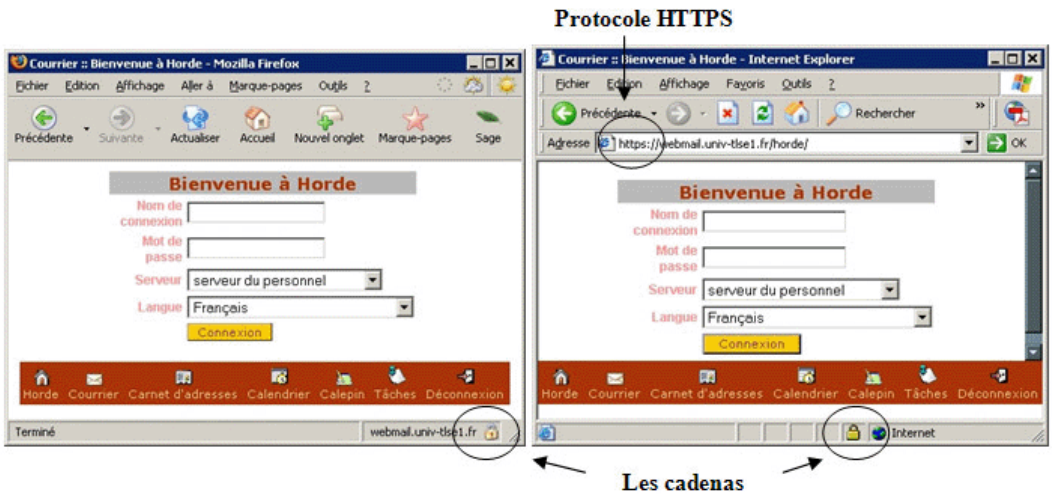
L'exemple ci-dessus peut faire rire mais il existe une technique d'arnaque plus inventive : le *phishing*.

Le but est d'extorquer à un internaute non averti des codes d'authentification de comptes bancaires ou des numéros de carte bleue. Pour obtenir ce genre de renseignement, l'escroc se fait passer pour un site de commerce électronique ou une banque dans lesquels il espère que l'internaute est client. Il reproduit une page web "factice" similaire aux couleurs de l'entreprise où le client est amené à entrer des informations personnelles telles que ses codes bancaires, sous prétexte d'une mise à jour ou bien que ceux-ci ont été maladroitement effacés par exemple. Sur la quantité énorme de courriers que l'escroc envoie, il tombe forcément sur une personne effectivement cliente de l'entreprise en question et naïve de surcroît.



Démarche

Se protéger de ce genre d'arnaques est très simple. Les banques n'envoient JAMAIS de courriers électroniques à leur client pour leur demander leur numéro de compte. Pour ce qui est des sites de commerce électronique, ne donnez de codes bancaires que lorsque vous êtes sur une page sécurisée. Une page sécurisée utilise le protocole https que l'on peut vérifier dans la barre d'adresse du navigateur en inspectant l'adresse. Un petit cadenas fermé dans la barre d'état du navigateur rappelle que les données transmises sont cryptées.



▲ IMG. 17 : PAGE SÉCURISÉE DANS IE ET FIREFOX

Partie B. Les canulars (hoax)

Définition des hoax



Hoax
Terme anglais qu'on peut traduire par canular, le hoax peut être défini comme une fausse information ou une rumeur. C'est une forme particulière de spam puisqu'il se base sur le courrier électronique. Il utilise la crédulité des utilisateurs pour se propager. En faisant circuler des informations qui apparaissent à l'utilisateur comme essentielles il compte sur celui-ci pour relayer (forwarder) l'information à tous ses contacts.

1. Exemples de canulars

La fausse alerte au virus

Ce soi-disant virus est en fait un fichier exécutable du système d'exploitation qui a toute son utilité. Heureusement cet exécutable n'était pas primordial pour le fonctionnement du système d'exploitation mais a tout de même causé quelques petites gênes.



Exemple
UN DE MES CORRESPONDANTS A ETE INFECTE PAR UN VIRUS QUI CIRCULE SUR LE MSN MESSENGER. LE NOM DU VIRUS EST jdbgmgr.exe L'ICONE EST UN PETIT OURSON. IL EST TRANSMIS AUTOMATIQUEMENT PAR MESSENGER AINSI QUE PAR LE CARNET D'ADRESSES. LE VIRUS N'EST PAS DETECTE PAR MC AFEE OU NORTON ET RESTE EN SOMMEIL PENDANT 14 JOURS AVANT DE S'ATTAQUER AU DISQUE DUR. IL PEUT DETRUIRE TOUT LE SYSTEME. JE VIENS DE LE TROUVER SUR MON DISQUE DUR ! AGISSEZ DONC TRES VITE POUR l'ELIMINER COMME SUIT : Très simple à faire ! 1. Aller à DEMARRER, faire "RECHERCHER" 2. Dans la fenêtre FICHIERS-DOSSIERS taper le nom du virus: jdbgmgr.exe 3. Assurez vous de faire la recherche sur votre disque dur "C" 4. Appuyer sur "RECHERCHER MAINTENANT" 5. Si vous trouvez le virus L'ICONE EST UN PETIT OURSON son nom "jdbgmgr.exe" NE L'OUVREZ SURTOUT PAS !!!!! 6.Appuyer sur le bouton droit de la souris pour l'éliminer (aller à la CORBEILLE) vous pouvez aussi l'effacer en appuyant sur SHIFT DELETE afin qu'il ne reste pas dans la corbeille. 7. Aller à la CORBEILLE et l'effacer définitivement ou bien vider la corbeille. SI VOUS TROUVEZ LE VIRUS SUR VOTRE DISQUE DUR ENVOYEZ CE MESSAGE A TOUS VOS CORRESPONDANTS FIGURANT SUR VOTRE CARNET D'ADRESSE CAR JE NE SAIS PAS DEPUIS QUAND IL EST PASSE.

La fausse chaîne de solidarité

Le message de cette chaîne de solidarité d'un fort mauvais goût a même été imprimé et distribué par des personnes croyant faire une bonne action.

Exemple

Bonjour à tous, Je vous sollicite car une petite fille de 9 mois doit être sauvée. Noélie est atteinte d'une leucémie rare. Le seul moyen pour que cette petite ne décède pas dans moins de 2 mois c'est que vous tous vous vous monopolisiez pour trouver un donneur compatible. Ce donneur doit être un homme de moins de 40 ans avec un groupe sanguin A Négatif. Je vous demande donc de bien vouloir communiquer à un maximum de gens cette information. D'avance merci à tous. les personnes à contacter : MME PATRICIA TANCE AU 02 32 xx xx xx EFS de BOIS GUILLAUME AU 02 35 xx xx xx

Exemple



▲ IMG. 18 : VOIR LES VERSIONS WEB POUR ACCÉDER AU FICHIER D'EXEMPLE (FICHIER POWERPOINT)

2. Stop aux canulars !

En général, le hoax n'est pas réellement dangereux puisqu'il ne met pas en défaut la sécurité des données de l'utilisateur et n'essaie pas de lui extorquer de l'argent. Cependant, le hoax possède quelques côtés pervers :

- Il sert la désinformation en faisant circuler de fausses informations ou des rumeurs non fondées et décrédibilise le moyen de diffusion que représente Internet.
- Il engorge les réseaux et les boîtes aux lettres en se servant des utilisateurs crédules pour être propagé.

Le site web www.hoaxbuster.com est une ressource en ligne recensant tous les hoax qui circulent sur Internet. Pour lutter contre la désinformation, pensez à toujours vérifier une information avant de l'envoyer à vos amis.

Conseil

- Une alerte de virus par email : mettez votre anti-virus à jour et laissez-le faire son boulot !
- Une chaîne de solidarité : vérifiez sur www.hoaxbuster.com !
- Votre souhait se réalisera ... arrêtez de lire l'horoscope, vous allez finir par y croire !

Partie C. Exercices - QCM

Exercice n°7. Info ou intox ?

Allez vérifier (sur hoaxbuster) si le texte suivant est un canular ou pas :

Le décret n° 2004-293XBS paru en début de mois au journal officiel relatif à la sécurité routière et modifiant le code de procédure pénale et le code de la route crée désormais une infraction spécifique à tout conducteur n'ayant pas signé le verso de la vignette d'assurance automobile sur le pare-brise, ainsi que la carte verte...
Pour éviter de payer l'amende de 180 euros en cas de contrôle, nous vous recommandons de vérifier la vignette d'assurance sur le pare-brise de votre véhicule.
Pour être valable, le verso de la vignette doit être obligatoirement signée par le souscripteur du contrat d'assurance.
Savez vous que 90% des conducteurs ont oubliés cette signature ? Et vous, y avez-vous pensé ?
Actuellement, la police du Nord de la France verbalise systématiquement les automobilistes 'tête en l'air' et parfois même 'tête à claques'. Devant ce gain facilement percevable, le ministre de l'intérieur a demandé d'étendre l'opération au territoire français.
Nous vous conseillons de relire votre contrat d'assurance automobile, vous constaterez qu'il existe un article (R. 69PQ) vous recommandant de signer le verso de la vignette d'assurance automobile.
La phrase stipule : 'La vignette a apposer sur le pare-brise n'est valable que si le verso est signé par le souscripteur du contrat d'assurance'.
Faites-le, vous ferez ainsi une économie de 180 euros.

Exercice n°8. Questions



Question1
Qu'est-ce qu'un hoax ?



Question2
Qu'est-ce qu'un spam ?



Question3
Citez deux formes dangereuses de spam.



Question4
Les sociétés commerciales ont-elles le droit d'utiliser le spam comme moyen de communication ?

Question5

Je n'arrête pas de recevoir des publicités d'une société que je ne connais pas.

- je me désabonne en cliquant sur le lien contenu dans le mail
- j'installe un anti-virus
- j'installe un anti-spam
- je réponds au mail en disant à la société de cesser les envois

Question6

Je reçois un mail avec un fichier attaché contenant de magnifiques photos de chats et se terminant par le message suivant : " si tu aimes les chats renvoi ce mail à tous tes amis ! "

- j'aime trop les chats je m'exécute
- j'évite de surcharger inutilement les boîtes aux lettres de mes amis
- je ne sais pas quoi faire

Chapitre

IV

Détecter un comportement anormal

Objectifs pédagogiques

Les trois chapitres précédents ont clairement démontré l'importance de la prévention, lorsqu'il s'agit de sécurité informatique. Pouvoir prévenir le danger limite considérablement le risque, encore faut-il pouvoir détecter un comportement anormal de l'ordinateur suffisamment tôt.

Le but de ce chapitre est que l'apprenant :

- Puisse identifier les comportements anormaux ou suspects de sa machine.
- Soit sensibilisé à l'observation critique de son environnement de travail.

Dans ce chapitre, nous considérerons uniquement les cas non critiques et causés par des intrusions malveillantes. En d'autres termes, nous ne parlerons pas des cas où l'ordinateur a été rendu inutilisable du fait d'une panne matérielle ou bien d'un virus qui aurait effacé le contenu des disques de l'ordinateur ou encore qui l'empêcherait de démarrer (*booter*).
Il existe deux éléments à surveiller : la machine elle-même et les logiciels.

Partie A. Comportement de la machine ou des périphériques

Comportement de la machine ou des périphériques

Le fonctionnement interne du micro-ordinateur est généralement et intentionnellement caché à l'utilisateur. Cependant, il existe plusieurs moyens de se faire une idée de l'activité de ses principaux organes vitaux.

- Des diodes placées sur le boîtier permettent de jauger l'activité du disque.
- Le Gestionnaire des tâches du système d'exploitation permet de lire l'activité du processeur et accessoirement le trafic réseau.

Le temps de réponse de l'ordinateur aux sollicitations de l'utilisateur permet de savoir si celui-ci est plutôt libre ou croule sous les opérations à effectuer.

Dès lors qu'il peut, grâce à ces indices et ces relevés, juger de l'activité de sa machine, l'utilisateur peut se demander si cette activité est réellement justifiée, compte tenu des opérations qu'il est en train de réaliser.

1. Réplication des vers ou des virus

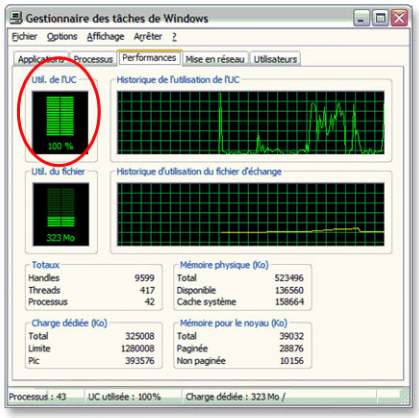
Le comportement anormal typique voit l'ordinateur soudainement débordé et incapable de répondre aux commandes de l'utilisateur : on dit qu'il rame.



Un ordinateur rame
En jargon informatique, un ordinateur rame si toutes ses ressources sont occupées et qu'il se trouve dans l'incapacité de répondre à l'utilisateur dans des délais raisonnables.

Il n'y a qu'une raison qui peut amener l'ordinateur à cet état, la gestion ou le lancement simultanés de plusieurs applications ou d'une seule application " gourmande en ressources ". Les conséquences sont une surcharge temporaire du processeur allant de pair avec une activité intense des disques durs. Ce phénomène, outre la perte d'interactivité avec le système d'exploitation, est facilement identifiable.

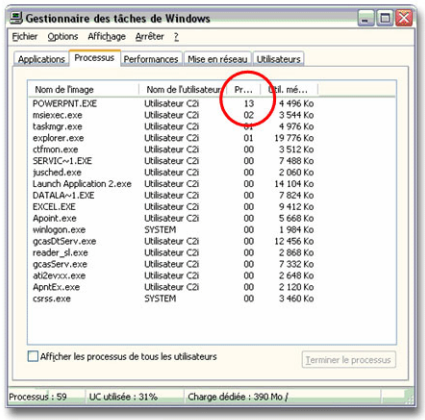
- La diode rouge sur le boîtier, dédiée au disque dur, rend compte de l'activité de celui-ci. Un clignotement rapide signifie une forte activité. Généralement, le bruit du disque dur permet également d'identifier un régime élevé.
- Ensuite, le Gestionnaire des tâches du système d'exploitation permet d'apprécier en temps réel l'utilisation du processeur.



▲ IMG. 19 : LE GESTIONNAIRE DES TÂCHES DE WINDOWS XP RÉVÈLE UNE CHARGE DU PROCESSEUR IMPORTANTE

Il est normal que l'ordinateur rame lorsqu'on utilise une ou plusieurs applications conséquentes. Par contre, si aucune des applications lancées ne le justifie a priori, un tel ralentissement devient anormal...

Les virus et les vers sont avant tout des programmes qui visent à se répliquer. Il n'est pas insensé de penser qu'une perte soudaine de performance puisse être attribuée à l'un d'eux. Afin de savoir si c'est réellement le cas, il existe une technique simple.
Le Gestionnaire des tâches du système d'exploitation permet de connaître en temps réel la liste des processus actifs du système et le temps de calcul qu'ils nécessitent. Il est donc aisé de repérer les processus à l'origine de ce ralentissement soudain et de les identifier.



▲ IMG. 20 : LE GESTIONNAIRE DES TÂCHES DE WINDOWS XP PERMET DE DÉTECTER LES PROCESSUS SUSPECTS

Lorsqu'une tâche qui monopolise le processeur possède un nom étrange, il peut s'agir d'un ver ou d'un virus. Le site http://www.processlibrary.com/ tient à jour la liste exhaustive de tous les processus de Windows et permet de lever rapidement le moindre doute.



Remarque

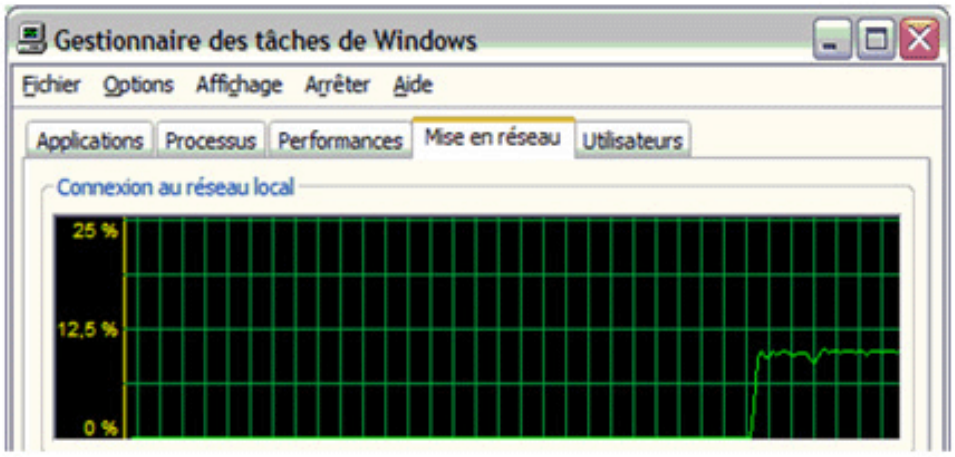
De manière générale, et même si les symptômes ne se font pas ressentir, la présence d'un virus actif dans l'ordinateur se traduit par la présence d'un processus associé. Tuer le processus empêche le virus d'opérer mais celui-ci se relancera automatiquement au prochain démarrage, tant qu'il n'aura pas été éradiqué par un logiciel de désinfection.

2. Propagation des vers ou des virus

Un autre comportement anormal est l'accès inexplicable aux ressources externes. Le plus facilement repérable est le lecteur de disquette pour son bruit peu discret.

Enfin, un troisième comportement anormal est le ralentissement du réseau, et plus spécifiquement de la connexion Internet. Celle-ci est visible lorsque l'affichage des pages web durant la navigation devient insupportablement lent pendant quelques minutes. Bien sûr, le chargement d'une page web contenant des ressources multimédia telles qu'une vidéo, un son, une animation flash ou un programme Java peut expliquer un tel ralentissement. De même, le fournisseur d'accès peut être à l'origine d'une baisse de débit mais celle-ci dure rarement moins d'une journée. Mais lorsque le ralentissement est soudain et les pages sont peu volumineuses, comment l'expliquer ?
De la même manière qu'un ver ou qu'un virus contamine le disque dur afin de se reproduire, il va essayer de contaminer les disques amovibles ou les ordinateurs en réseau afin de se propager. On peut imaginer que ce phénomène puisse être à l'origine d'un accès suspect au lecteur de disquette ou bien d'une baisse de débit significative et temporaire.

Remarque
Si le virus tente d'infecter les disques amovibles et de se propager sur d'autres machines par le réseau ou par Internet, il est fort probable que le disque dur de l'ordinateur soit déjà totalement infecté.



▲ Img. 21 : Le Gestionnaire des tâches de Windows XP montre clairement une forte augmentation de l'utilisation du réseau

Partie B. Fonctionnement anormal des logiciels

Préambule

Nous avons vu que le fonctionnement de l'ordinateur peut délivrer un certain nombre d'informations et éventuellement révéler la présence d'un virus ou d'un ver. Les logiciels également peuvent aider l'utilisateur dans ce sens.

1. Prise de contrôle de l'ordinateur

Premier logiciel de l'ordinateur, le système d'exploitation contrôle tous les autres. En outre, il est seul capable de lancer les applications, les fermer, les basculer en plein écran ou les réduire. On peut considérer comme comportement suspect toute opération qui n'a pas été explicitement commandée par l'utilisateur. Contrairement au comportement de la machine, la perte de contrôle du système d'exploitation ne laisse plus aucun doute !

Lorsque les logiciels agissent selon leur gré, il est en effet pratiquement certain qu'un virus ou un ver infecte la machine et se soit déclenché. Ce n'est généralement qu'après avoir infecté la machine et s'être propagé sur l'ensemble du disque et des ressources

disponibles que le virus devient actif et prend le contrôle de la machine afin d'exécuter la tâche pour lequel il a été conçu. Dans certains cas, cela consiste simplement à ouvrir automatiquement des pages web illégales. De plus, il est possible que le virus soit en mesure de fermer automatiquement tout logiciel anti-virus dès que l'utilisateur tente de scanner l'ordinateur. Il faut dans ce cas tuer le processus associé au virus avant de tenter une désinfection.



Remarque

Si le virus entre en activation et commence à prendre le contrôle de la machine, il est certain qu'il s'est déjà propagé sur les autres ordinateurs du réseau et tous les supports avec lesquels il est entré en contact. Isolez chaque machine avant d'essayer de la désinfecter.

2. Détournement

Parmi les comportements étranges directement observables, on peut également citer ceux qui touchent le navigateur Internet.

Par exemple le changement de la page de démarrage : au lieu de démarrer sur votre page d'accueil habituelle, le navigateur ouvrira la page principale d'un site à caractère promotionnel ou pornographique.
Le navigateur peut également détourner systématiquement toutes les pages que l'utilisateur visite durant la navigation et l'amener sur des sites illégaux. Ce cas est plus grave car l'utilisateur n'a pratiquement plus aucun contrôle sur la navigation.
Enfin, la navigation peut également être perturbée soudainement et de manière durable par l'affichage de dizaines de pop-ups, quels que soient les sites que l'utilisateur visite.
Si les vers ou les virus se propagent par les fichiers, les spywares s'attrapent sur Internet grâce à des failles du navigateur. Une perte de contrôle ou un changement irréversible des paramètres de celui-ci trahit donc son infection par un logiciel espion.
L'infection du navigateur Internet est moins grave que celle du système d'exploitation mais constitue néanmoins une menace pour les données de l'utilisateur.

Partie C. Exercices - QCM

Exercice n°9. Questions



Question1

J'étais en train de travailler de travailler avec Word et Excel tout en ayant mon logiciel de messagerie ouvert. J'ai décidé de lancer l'explorateur Internet et ce programme a mis plusieurs dizaines de secondes pour s'ouvrir.
Comment savoir si un virus est présent sur ma machine et la ralentit ?



Question2
Alors que je suis en train de lire mes mails sur mon logiciel de messagerie, la diode rouge située sur le boîtier ne cesse de clignoter et j'entends le disque dur qui crépite.
Que se passe-t-il ?



Question3
Mon ordinateur essaie d'accéder au lecteur de disquette. Pourtant il n'y a pas de disquette à l'intérieur.
Qu'est-ce que cela veut dire ?



Question4
Depuis hier, j'ai beaucoup de mal à naviguer sur Internet car l'affichage des pages est excessivement lent. Est-ce dû à un virus ?



Question5
A intervalles réguliers, mon navigateur Internet se lance sans que je ne l'aie demandé. Lorsque je le ferme, il se réouvre quelques minutes plus tard. A quoi est-ce dû ?



Question6
Le gardien de mon anti-virus m'a alerté de la présence d'un virus sur ma machine mais lorsque je lance le scanner, celui-ci s'arrête au bout de quelques secondes.
Que faire ?



Question7
Lorsque je lance mon explorateur Internet, celui-ci m'affiche une page appartenant à un site pornographique ou publicitaire. J'ai beau changer ma page d'accueil, la page indésirable revient constamment.
Comment faire pour remettre ma page d'accueil initiale de manière durable ?



Question8
Comment se fait-il que lorsque je tape l'adresse d'un site dans la barre d'URL du navigateur Internet, celui-ci m'oriente vers un autre site à caractère promotionnel ou pornographique ?

* *
*

La hausse des dangers que représentent les virus, les vers, les logiciels espions et des nuisances causées par le pourriel est essentiellement imputable à l'utilisateur lui-même. Par le biais de sa méconnaissance des dangers d'Internet, de sa crédulité et de son incapacité à pouvoir diagnostiquer un comportement anormal de sa machine, celui-ci se retrouve souvent complice involontaire.

Chapitre

V

Assurer une sauvegarde (sur le réseau, support externe,...)

Objectifs pédagogiques

Le but de chapitre est que l'apprenant :

- Connaisse les règles élémentaires de sauvegarde.
- Sache effectuer une sauvegarde.

Partie A. Pourquoi, quand, quoi, ... ?

1. Pourquoi faire une sauvegarde ?

Comme nous l'avons vu dans le premier chapitre, la perte de données, quelle qu'en soit la cause, est la principale raison pour faire une sauvegarde.

Mais d'autres situations peuvent inciter l'utilisateur à faire une sauvegarde :

- Avant l'installation d'un nouveau logiciel afin de pouvoir revenir en arrière en cas de problème.
- Avant une intervention technique sur votre machine qui peut endommager le système.

2. Quelle fréquence de sauvegarde ?

L'utilisateur doit adopter un rythme de sauvegarde en fonction du caractère sensible de ses données et du rythme de modification.

S'il travaille très régulièrement sur les mêmes fichiers, il est nécessaire de faire une sauvegarde très régulièrement de ceux-ci afin d'éviter, en cas de perte, d'avoir à refaire un trop grand nombre de modifications.
Si les données ont un caractère sensible (par exemple : les informations de tous les clients d'une entreprise, les commandes en cours, etc.), elles doivent être sauvegardées très souvent car une perte de celles-ci pourrait avoir des conséquences néfastes (par exemple : la faillite de l'entreprise).

3. Que doit-on sauvegarder ?

Cela dépend de l'environnement (professionnel ou privé) et de l'importance que ces données présentent.

Pour répondre à cette question, supposons que le disque dur de l'utilisateur tombe en panne et qu'il n'ait aucun moyen de récupérer les informations :

- Quelles données a-t-il définitivement perdues ? Ses photos de vacances, ses emails personnels, un rapport important, etc.
- Quelles sont celles qui lui sont utiles à court terme ? Ses favoris, ses adresses emails et numéros de téléphone de ses amis, collègues ou clients, etc.

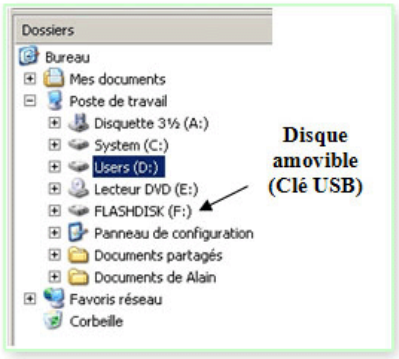
Partie B. Des méthodes de sauvegarde

Dans ce paragraphe, nous allons voir différentes méthodes de sauvegarde.

1. Simple copie sur support amovible

La manière la plus courante de préserver des données est d'effectuer une sauvegarde sur un support amovible (CD-ROM, ZIP, JAZ, clé USB).

Après avoir inséré le support celui-ci apparaît comme un nouveau disque amovible disponible sur votre machine, il suffit ensuite de faire, par exemple, une simple copie des répertoires à sauvegarder.



▲ IMG. 22 : LISTE DES DISQUES DISPONIBLES

Cette façon de faire est très simple mais elle a trois défauts majeurs :

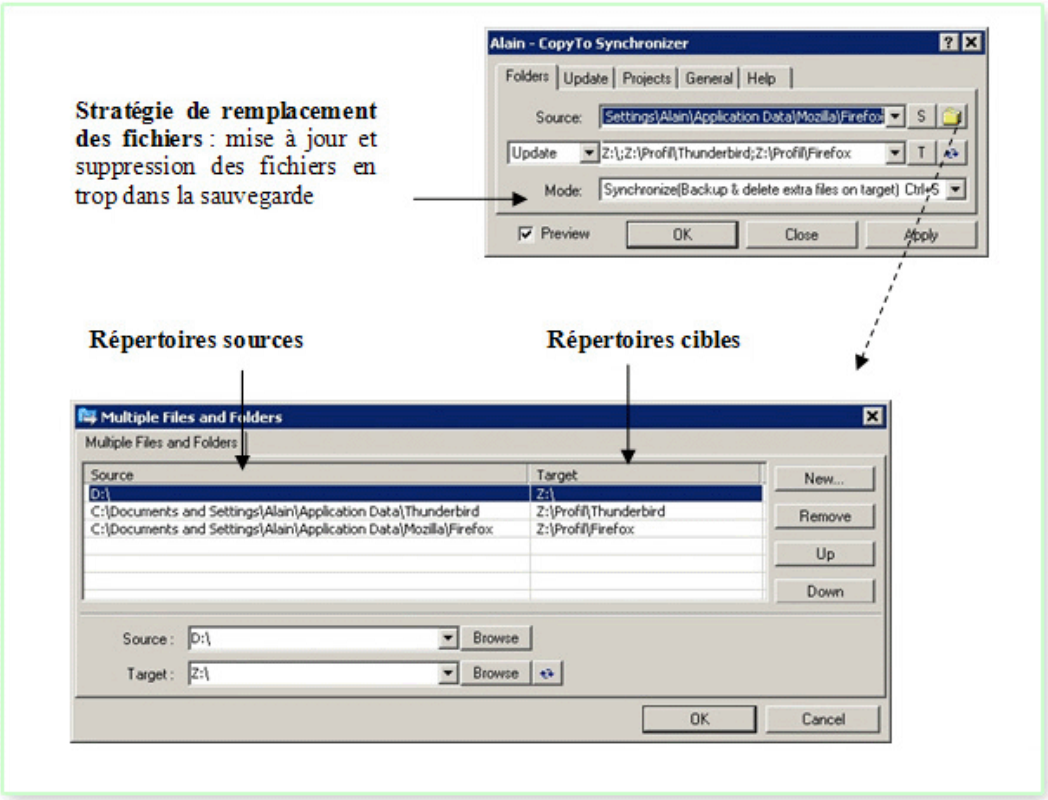
- L'utilisateur doit penser à renouveler cette action relativement souvent.
- Si ses données sont réparties dans un nombre de répertoires important, il peut arriver d'oublier de sauvegarder certains d'entre eux.
- Les données sont recopiées systématiquement même celles qui n'ont pas changées. Cela utilise de la place de manière excessive et augmente le temps passé à faire la sauvegarde.



Démarche

Pour remédier au premier problème, on peut mettre en place un système de sauvegarde automatique. La mise en oeuvre de celle-ci va dépendre du système d'exploitation mais aussi du logiciel utilisé pour faire la sauvegarde.

Par contre les deux derniers problèmes peuvent être résolus en utilisant un logiciel permettant d'enregistrer des profils de sauvegarde et offrant la possibilité de comparer les données que l'on souhaite mettre à jour avec les données contenues dans la sauvegarde. Ainsi, seuls les fichiers et répertoires modifiés seront changés.



▲ IMG. 23 : COPYTO, UN LOGICIEL PERMETTANT DE SYNCHRONISER PLUSIEURS RÉPERTOIRES SIMULTANÉMENT (HTTP://WWW.NE.JP/ASAHI/COOL/KISH/)

2. Le mirroring

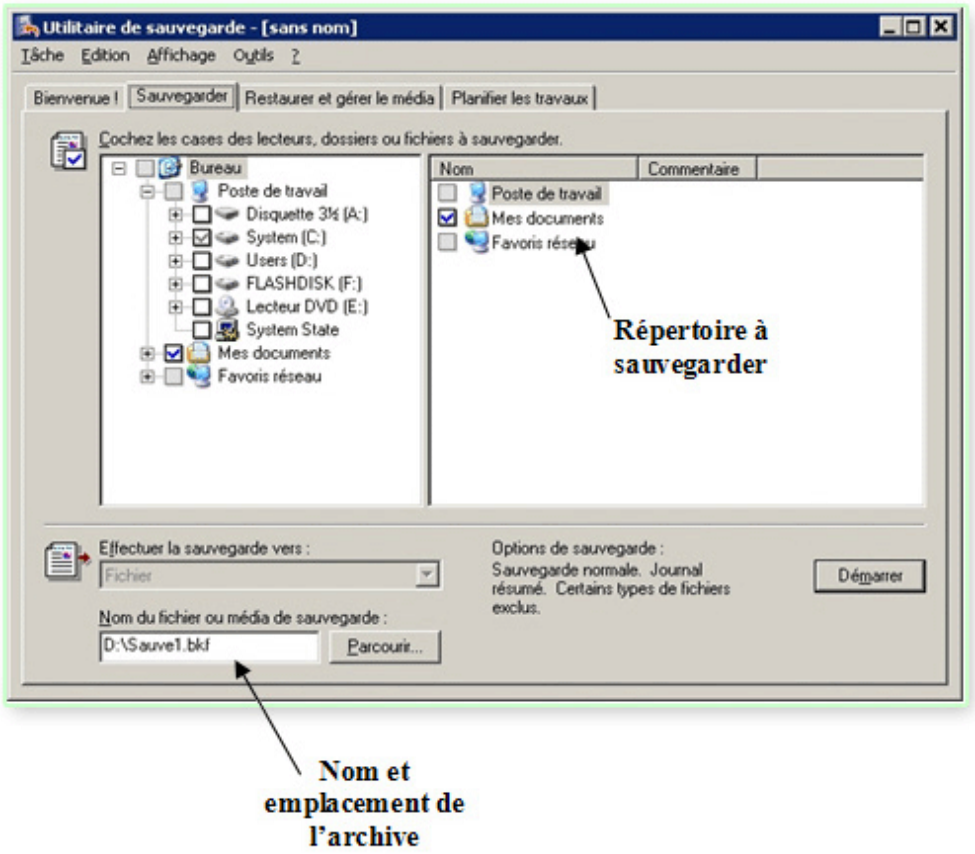
Le mirroring (ou *disque en miroir*) a pour but de dupliquer l'information à stocker sur plusieurs disques simultanément. Ce procédé est basé sur la technologie RAID (acronyme de Redundant Array of Inexpensive Disks, traduire ensemble redondant de disques indépendants) qui permet de constituer une unité de stockage à partir de plusieurs disques durs.

L'unité ainsi créée (appelée *grappe*) a une grande tolérance aux pannes et possède une haute disponibilité. En effet, on obtient ainsi une plus grande sécurité des données, car si l'un des disques tombe en panne, les données sont sauvegardées sur l'autre. D'autre part, la lecture peut être beaucoup plus rapide lorsque les deux disques sont en fonctionnement. Enfin, étant donné que chaque disque possède son propre contrôleur, le serveur peut continuer à fonctionner même lorsque l'un des disques tombe en panne, au même titre qu'un camion pourra continuer à rouler si un de ses pneus crève, car il en a plusieurs sur chaque essieu.
En contrepartie ce procédé est très onéreux étant donné que seule la moitié de la capacité de stockage est utilisée de manière effective.

3. Le backup

Les logiciels de " backup " proposent de sauvegarder un ensemble de fichiers et de répertoires dans un fichier appelé archive. Ils offrent en général un grand nombre de fonctionnalités :

- Archivage et récupération des données.
- Compression des données.
- Planification des sauvegardes.
- Choix des différents répertoires et fichiers à sauvegarder.
- Choix de l'emplacement de l'archive : disque amovible, disque réseau,...



▲ IMG. 24 : BACKUP SOUS WINDOWS XP PRO

Chapitre

VI

Compresser/décompresser ses données

Objectifs pédagogiques

Le but de ce chapitre est de :

- Connaître le principe de la compression/décompression de données et de l'archivage de données.
- Identifier les principaux formats de compression.
- Savoir la différence entre une compression sans perte ou avec perte.

Partie A. Introduction

Définitions



Compresser
Compresser, c'est l'action de réduire la taille d'un fichier en modifiant le codage de l'information. Après la compression le fichier n'est donc plus lisible par le logiciel qui a servi à le créer et il change d'extension. Avant de pouvoir le réutiliser il faut le décompresser c'est-à-dire lui faire reprendre sa taille et son codage d'origine de façon à reconstruire l'information initiale.



Codec
Codec, abréviation de compresseur/décompresseur. Élément logiciel ou matériel permettant de compresser et de décompresser des données multimédias numériques.



▲ IMG. 25 : COMPRESSER / DÉCOMPRESSER

1. Pourquoi a-t-on besoin de compresser les données ?

Le besoin de compression apparaît là ou la taille du fichier a un caractère critique. Par exemple :

- Lors de l'envoi de courrier électronique, les fournisseurs d'accès limitent la taille des fichiers attachés pour éviter d'encombrer les boites aux lettres. La compression permettra de réduire la taille de vos fichiers et donc de pouvoir les envoyer.
- La création d'image numérique est très coûteuse en mémoire car pour avoir une image de bonne qualité il faut qu'elle ait une définition importante et une palette de couleur assez grande. Le problème est identique pour les fichiers vidéos ou sonores. Donc la plupart des formats d'enregistrement des fichiers numériques multimédia sont des formats utilisant la compression.
- Lors de la sauvegarde sur un support externe, il est très utile de pourvoir réduire la taille totale des données à sauvegarder afin de gagner en place et temps de sauvegarde.

2. La taille des fichiers

Pour connaître la taille occupée par un fichier il y a plusieurs solutions :

1. Ouvrez le fichier puis faites Fichier/Propriétés dans l'application.
2. Sélectionnez le fichier dans le gestionnaires de fichiers puis faites Fichier/Propriétés.
3. Dans le gestionnaire de fichiers, faites apparaître le menu contextuel du fichier puis cliquez sur propriétés.

Il y a 2 tailles différentes indiquées dans les propriétés :

- La taille réelle qui correspond à la taille effective de votre fichier.
- La taille occupée sur le disque qui dépend de la taille des clusters de votre disque dur.

Partie B. Compresser et décompresser un fichier et/ou un répertoire

Définitions

Archive

Une archive est un fichier souvent compressé qui comporte plusieurs autres fichiers et/ou répertoires.

Archiver

Archiver signifie que l'on regroupe dans un seul fichier un ensemble de fichiers et/ou de répertoires. Lorsque vous ajoutez un répertoire à une archive les fichiers et les sous-répertoires qu'il contient sont également ajoutés.



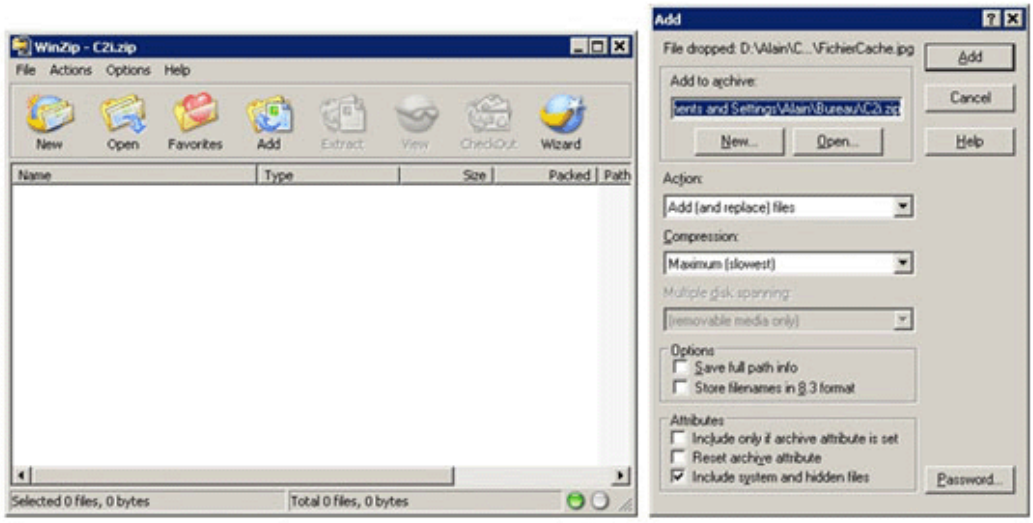
▲ IMG. 26 : ARCHIVER / DÉSARCHIVER

1. Création d'une archive avec Winzip

Démarche

Pour créer une archive avec Winzip 8 :

- Lancer le logiciel.
- Demander la création d'une nouvelle archive.
- Donner un nom à cette archive.
- Ajoutez un ou plusieurs fichier(s) et/ou répertoire en le(s) glissant dans la fenêtre de l'archive.



▲ IMG. 27 : ARCHIVE VIDE À GAUCHE ET BOÎTE DE DIALOGUE ADD À DROITE DE WINZIP 8

Explication

Description de la boîte de dialogue " Add "

- **Action :**

  permet de définir la stratégie d'ajout des fichiers à l'archive (remplacement, mise à jour, etc.)

- **Compression :**

  permet de définir le taux de compression, plus la taux de compression est élevé plus le temps d'ajout du fichier est long et inversement.

- **Password :**

  permet de définir un mot de passe sur un fichier pour empêcher sa décompression par des personnes non autorisées.

Partie C. Les divers formats de compression (zip, rar, gzip, tar, ...)

1. Formats de compression : définitions

Ces formats de compression utilisent une compression physique sans perte d'information car le but de ces formats de compression est simplement de réduire la taille de l'ensemble des fichiers.



Compression physique
La compression physique agit sur les bits, sans savoir quel type de donnée elle manipule. De plus elle est sans perte d'information.



Compression sans perte
La compression sans perte d'informations assure que la donnée une fois décompressée sera identique à l'originale ayant servi à la compression.

Il existe plusieurs formats de compression, parmi les plus connus : ZIP, son homologue GZIP (GNU ZIP) et le format RAR qui se veut plus puissant. Tous les formats de compression physique sans perte sont néanmoins basés sur le même principe.

Des séquences redondantes sont identifiées dans la longue liste de bits que constitue un fichier. A chaque séquence est attribué un code, les codes les plus courts étant attribués aux séquences les plus fréquentes, selon le principe de Hufmann. En remplaçant des séquences de bits (du fichier original) par d'autres séquences mais plus courtes (codes), on diminue la taille du fichier. Au bout du fichier compressé, on rajoute le dictionnaire qui contient les codes ainsi que les séquences équivalentes, afin de permettre la décompression.

Partie D. La compression des images, du son et des vidéos

Définitions

La plupart des formats images, sons et vidéos utilisent une compression logique avec perte d'informations.



Compression logique
La compression logique utilise un algorithme (procédé) qui agit sur les données de manière spécifique.

En fonction du réglage de l'algorithme la compression peut se faire avec ou sans perte d'informations. Lors de la compression avec perte, la donnée reconstruite sera plus ou moins proche de la donnée originale en fonction de taux de compression utilisé. Mais

il n'est pas évident qu'une personne puisse faire la différence.

Exemple
Les deux photos ci-dessous vous paraissent identiques. Observez bien celle de droite est légèrement dégradée. Pourtant le taux de compression est important car l'image de gauche fait 92 Ko alors que celle de droite ne fait que 19 Ko.



▲ IMG. 28

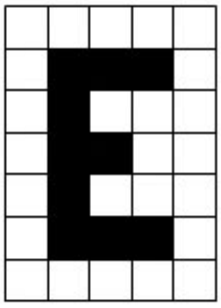
1. Les formats d'images

A chaque format d'image correspond un codage spécifique de l'information et éventuellement un algorithme de compression.

a) Comprendre la compression d'image.

Pour comprendre, il faut d'abord savoir comment est codée une image.

Une image est constituée d'un ensemble de points appelés pixels (pixel est une contraction de PICture ELement) Le pixel représente ainsi le plus petit élément constitutif d'une image numérique.



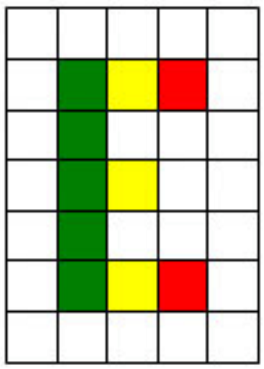
▲ IMG. 29 : LETTRE E EN PIXEL

Donc pour décrire une image il faut décrire l'ensemble de ses pixels et surtout la couleur de chacun deux. Si l'on considère que 1 équivaut à un pixel blanc et 0 à un pixel noir voici le code numérique simplifié en BMP de notre image (longueur : 35 caractères).

7, 5, 11111100011011110011101111000111111

Les deux premiers chiffres correspondent à la taille de l'image : 7x5 pixels.

Maintenant introduisons de la couleur avec une colonne en vert, une en jaune et une rouge.



▲ IMG. 30 : LETTRE E EN COULEUR

Pour arriver à définir correctement le spectre de couleur il faut utiliser une représentation dite RGB (Red, Green, Blue). Dans cette représentation la rouge a le code 100, le jaune 110, vert 010 et le blanc 111. Le code numérique de notre image est donc :

1111111111111111110101101001111110101111111111110101101111111111010111111111111

Nous voyons immédiatement que le fait d'ajouter de la couleur a considérablement augmenté la taille du code de l'image (longueur : 105 caractères).

b) Exemple d'un algorithme de compression sans perte : LZW

LZW, inventé par Lempel, Ziv et Welch, est un algorithme très rapide aussi bien en compression qu'en décompression, basé sur la multiplicité des occurrences de séquences de caractères dans la chaîne à encoder. Son principe consiste à substituer des motifs par un code d'affectation (indice) en construisant au fur et à mesure un dictionnaire.

De plus, il travaille sur des bits et non sur des octets, il ne dépend donc pas de la manière dont le processeur code l'information. C'est un des algorithmes les plus populaires, il est notamment utilisé dans les formats TIFF et GIF. La méthode de compression LZW a été brevetée par la société *Unisys* .



Explication

Chercher des séquences qui se répètent dans la lettre E afin de créer un dictionnaire. En déduire ensuite le nouveau codage de l'image. Calculer le ratio.
On profite du fait que la lettre E soit verticalement symétrique.
0 : 111111111111111 (Première et dernière lignes de la lettre)
1 : 111010110100111 (Deuxième et sixième lignes de la lettre)
2 : 111010111111111 (Troisième et cinquième lignes de la lettre)
3 : 111010110111111 (Quatrième ligne de la lettre)
Le code : 0123210
Si nous ajoutons le nombre de caractères (la ponctuation est négligée) utilisés pour le dictionnaire et pour le code nous arrivons à une taille de 64 + 7 = 71 caractères soit une compression sans perte de 33% (71*100/105).

BMP

Le format BMP est un format sans compression développé conjointement par Microsoft et IBM, ce qui explique qu'il soit particulièrement répandu sur les plates-formes Windows et OS/2. Un fichier BMP est un fichier bitmap, c'est-à-dire un fichier d'image graphique stockant les pixels sous forme de tableau de points et gérant les couleurs soit en couleur vraie soit par une palette indexée de couleurs.

GIF (Graphic Interchange Format)

Une image GIF peut contenir de 2 à 256 couleurs (2, 4, 8, 16, 32, 64, 128 ou 256) parmi 16.8 millions dans sa palette. Ainsi grâce à cette palette limitée en nombre de couleurs (et non limitée en couleurs différentes), les images obtenues par ce format ont une taille généralement très faible. Ce format supporte la compression LZW.

Le format Gif 87a offre une fonction d'entrelacement permettant d'afficher l'image progressivement et la possibilité d'enregistrer des images animées (GIF animés) et le format Gif 89 ajoute la possibilité de définir une couleur transparente très utile lors de la superposition d'images.



Exemple

Si nous reprenons le lettre E en couleur, la palette de couleurs sera constituée par quatre entrées : 0 pour le blanc (111), 1 pour le vert (010), 2 pour le jaune (110) et 3 pour le rouge (100).
Le code de la lettre E en format GIF est donc :
00000012300100001200010000123000000
Ce qui est nettement plus court que le code BMP.

JPEG

Développé par le Joint Picture Expert Group au cours des années 1980, le format JPEG ou JPG reste aujourd'hui un standard. Bien qu'avec perte, ce format peut gérer un taux de compression afin de définir la qualité de l'image compressée. Il n'impose aucune limitation dans le nombre de couleurs de l'image, ce qui en fait le format de prédilection pour compresser les photos ou les images de 32 bits (16 millions du couleurs).

Le processus de compression est très complexe et s'effectue en plusieurs passes. Il est basé sur la transformée en cosinus discrète (DCT), une formule mathématique dérivée

de la transformée de Fourrier, appliquée à des blocs de pixels. Les paramètres de cette fonction mathématique font office de taux de compression et permettent d'obtenir des rapports allant de 20:1 à 25:1.

PNG (Portable Network Graphics)

Le format PNG est un format de fichier graphique bitmap. Il a été mis au point en 1995 afin de fournir une alternative libre au format GIF, format propriétaire dont les droits sont détenus par la société Unisys, propriétaire de l'algorithme de compression LZW.

Le format PNG permet de stocker des images en noir et blanc, en couleurs réelles ainsi que des images indexées faisant usage d'une palette de 256 couleurs. .
De plus, il supporte la transparence par couche alpha, c'est-à-dire la possibilité de définir 256 niveaux de transparence, tandis que le format GIF ne permet de définir qu'une seule couleur de la palette comme transparente. Il possède également une fonction d'entrelacement permettant d'afficher l'image progressivement.
La compression proposée par ce format est une compression sans perte meilleure que la compression GIF

TIF (Tagged Image File Format)

Le format TIF ou TIFF est un format de fichier graphique bitmap mis au point en 1987.

Le format TIFF est un ancien format graphique, permettant de stocker des images bitmap de taille importante (plus de 4 Go compressées), sans perte de qualité et indépendamment des plates-formes ou des périphériques utilisés.
Le format TIFF permet de stocker des images en noir et blanc, en couleurs réelles ainsi que des images indexées faisant usage d'une palette de couleurs.

2. Les formats audios

WAV

Le format WAV est l'équivalent audio du format Bitmap. Également développé par IBM, il reprend le principe de la compression minimale. Pour simplifier, on peut dire que le WAV encode directement le son numérisé, sans aucune forme de compression, ce qui tend à produire des fichiers de taille conséquente. Pour cette raison, les fichiers WAV sont uniquement destinés aux sons très courts (tels que les jingles de Windows par exemple). Pour les fichiers musicaux plus long, on lui préfère indéniablement le format MP3.

MP3

Le MP3 " MPEG Audio layer 3 " est un format de compression de données audio par filtrage des données audio. Ce format permet de compresser à un taux de 1:12 les formats audio habituels (WAV ou CD audio). Il permet de faire tenir l'équivalent en fichiers de douze albums de musique sur un seul cd-rom. De plus, le format MP3 n'altère que faiblement le son pour l'oreille humaine.



Remarque

Le format MP3 n'est pas illégal car il représente uniquement une façon de compresser des données numériques. Par contre son utilisation peut l'être. Lors de l'utilisation de fichiers MP3, veillez à respecter les droits d'auteur. Le principe d'exception de copie privée prévoit qu'il est possible de posséder une copie numérique d'une oeuvre musicale à condition que l'on possède l'original (sur CD par exemple) mais vous ne pouvez pas télécharger ou archiver une musique d'un artiste dont les droits d'utilisation ne sont pas libres de droit. Il est ainsi fort peu probable que la chanson que vous rêvez de télécharger puisse légalement l'être.



Attention

Les oeuvres numérisées sont réservées à un usage privé (cercle familial ou d'amis).

La diffusion de ces fichiers en dehors de ce cadre (mise à disposition sur un réseau peer-to-peer, un site web ou FTP, envoi par courrier électronique, etc.) est strictement interdite.

OGG

Le format OGG (Ogg Vorbis) est une alternative au format MP3 qui est censée produire des fichiers de bien meilleure qualité pour une taille toutefois légèrement supérieure. Réclamé par les audiophiles qui jugent la compression MP3 trop drastique, il est développé en tant que logiciel libre, à l'inverse des formats MP3, AAC et WMA.

AAC

Le format AAC, développé par le Moving Picture Expert Group, a pour but de remplacer le MP3, prévu originellement pour accompagner les vidéos MPEG-1. Celui-ci gère le son des fichiers MPEG-4 et doit offrir une qualité bien meilleure que le MP3 et gérer plus de canaux.

3. Les formats vidéos

AVI (Audio Video Interleaved)

Format de fichier utilisé par Windows pour le stockage des images vidéos et du son, dans lequel les données vidéos alternent avec les données audios, accélérant ainsi la vitesse de restitution. Dans ce format, on dit que l'image et le son sont entrelacés.

MPG, MPEG2, MPEG4

Format multimédia obtenu par la compression MPEG ou MPG de séquences audios et vidéos.

Le format MPEG-1 est d'une qualité équivalente au VHS des magnétoscopes. Sur le Web, il permet une meilleure représentation numérique des séquences audios et vidéos que les autres formats disponibles (AVI, Indeo, QuickTime, etc.).
Le format MPEG-2, quant à lui, est utilisé pour le stockage de la vidéo et de l'audio sur DVD et la diffusion par les réseaux de télévision.
Le MPEG-4 par ses possibilités de compresser très efficacement la vidéo est parfois vu comme le " MP3 de la Vidéo ". Cela explique la confusion de ceux qui utilisent parfois le terme impropre MP4 au lieu de MPEG-4. Il intègre les formats 2D et 3D, et permet

une diffusion en streaming pour le bas et le haut débit.

DIVX
Le format DivX est un format de compression/décompression vidéo permettant d'obtenir des vidéos compressées très peu volumineuses avec une perte de qualité très raisonnable. Ainsi le format DivX permet de stocker un film complet sur un CD-ROM de 650 ou 700 Mo.

Les formats XVID, VP3, 3IVX sont des formats dérivés du DIVX.

Partie E. Exercices - QCM

Exercice n°10. Compression et Archivage

Compression et Archivage

Enoncé :

1. Créer à l'aide de Paint, un document DESSIN.BMP (dessiner rapidement quelque chose).

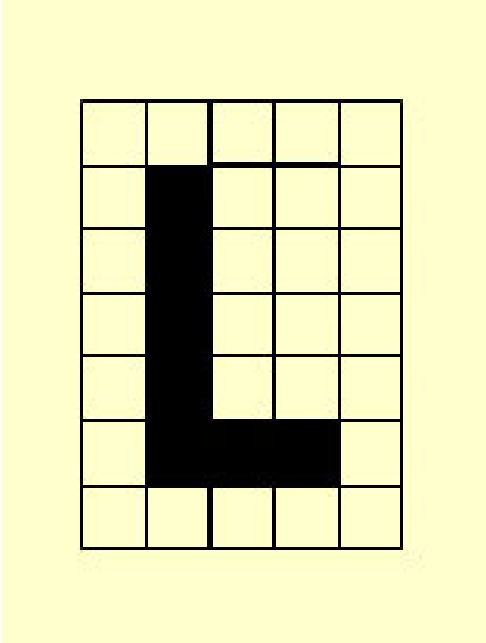
   Enregistrer ce document en format jpg et en format tiff (menu Enregistrer sous).
2. Comparer maintenant les tailles de ces trois fichiers.
3. Quel type de compression venez-vous d'appliquer ?
4. Compresser le fichier DESSIN.BMP à l'aide de WinZip.
5. Comparer la taille du fichier original et du fichier compressé. Quel est le taux de compression ? Quel est le gain de place ?
6. Compresser le fichier DESSIN.JPG en dessin1.zip. Comparer la taille du fichier original et du fichier compressé. Quel est le taux de compression ? Quel est le gain de place ?
7. Compresser le fichier DESSIN.JPG en dessin2.zip. Comparer la taille du fichier original et du fichier compressé. Quel est le taux de compression ? Quel est le gain de place ?
8. En admettant que j'ai un fichier de format de base jpg, quelle compression vaut-il mieux appliquer à ce fichier ?
9. Compresser le fichier dessin.zip. Quel est le gain de place ?
10. Archiver les trois fichiers zip dessin.zip, dessin1.zip et dessin2.zip en une seule archive archive_dessin.zip.

Exercice n°11. L, tu prends trop de place !

Donnez le codage numérique de la lettre L.

Proposez une compression sans perte de cette lettre en donnant le dictionnaire et le nouveau codage.

Citez des contextes dans lesquels la taille des données a un caractère critique.
Donnez la définition d'une archive ; Donnez la définition de la compression physique ; Donnez la définition de la compression logique.
Donnez 3 formats d'images. Donnez 3 formats audios. Donnez 3 formats vidéos.
Quelle est l'utilité de la compression avec perte ?



▲ IMG. 31

Exercice n°12. Questions

Question1
Citez des contextes dans lesquels la taille des données a un caractère critique.

Question2
Donnez la définition d'une archive.

Question3
Donnez la définition de la compression physique.

Question4
Donnez la définition de la compression logique.

Question5
Donnez 3 formats d'images.

Question6
Donnez 3 formats audios.



Question7
Donnez 3 formats vidéos.



Question8
Quelle est l'utilité de la compression avec perte ?

Synthèse

Chapitre final

La meilleure façon de se protéger est de vivre en vase clos : pas de connexion réseau, pas lecteur de disquette, pas de lecteur de cd-rom, pas de clé USB, etc. Bienvenus dans un monde de paranoïaques !
Soyons sérieux, le grand attrait de l'informatique est lié à Internet et à cette capacité de communiquer librement, facilement et d'avoir accès à une masse impressionnante d'informations. Un ordinateur sans connexion Internet est une voiture sans essence il ne vous mènera pas bien loin.
Alors prenons des risques, connectons nous ! Apprenons à conduire et allions un comportement prudent et vigilant !
Et cette masse d'informations, critiquons-la ! Domptons-la ! Elle nous sera bénéfique !

Glossaire

craquer (un mot de passe)

Casser, découvrir, trouver

hacker

Aujourd'hui, ce terme désigne un pirate des réseaux.
Le hacker s'introduit frauduleusement sur des systèmes informatiques, par le biais d'Internet, pour le défi, pour dérober des informations, pour s'accaparer des ressources, etc.

spam

Un spam est un courrier indésirable (voir partie IV).

cookie

Le cookie est un fichier texte de quelques kilo-octets seulement, dont le nom reprend celui de l'utilisateur et du site (ex: utilisateur@site.fr.txt). Il est localisé dans le répertoire destiné aux fichiers temporaires Internet.

plugin

Un plugin est une extension d'une application qui permet d'y ajouter de nouvelles fonctionnalités.
Par exemple, un navigateur Internet a besoin d'un plugin pour lire certains contenus audios/vidéos qui ne sont pas pris en charge d'origine.

opt-in

L'opt-in désigne le consentement préalable d'un internaute avant de lui envoyer de la publicité. C'est la règle qu'a retenu la loi sur l'économie numérique en matière de spam. Elle s'oppose à l'opt-out où l'internaute est inscrit d'office sur les listes de diffusion et doit se désinscrire manuellement s'il ne désire plus recevoir de publicité.

prospection directe

" Est interdite la prospection directe, notamment la publicité, au moyen de courriers électroniques utilisant, sous quelque forme que ce soit les coordonnées d'une personne physique ou morale non inscrite au registre du commerce et des sociétés qui n'a pas exprimé son consentement préalable à recevoir de tels courriers électroniques ".
Article 12 de la loi sur l'économie numérique

https

Contraction de HTTP, le protocole de transport, et de SSL (Secure Socket Layer), système qui permet d'échanger des informations entre 2 ordinateurs de façon sûre.

cluster

Espace minimum occupé par un document sur le disque dur. La taille de cet espace est choisie lors du formatage du disque dur.

filtrage

Le but du filtrage est d'enlever les bandes de fréquences pauvres en informations auditives.

streaming

Le streaming est une technique permettant le téléchargement et l'écoute simultanée d'un fichier audio et/ou vidéo.