

Diapo 3 (2005) Introduction

- **Le courrier électronique et le World Wide Web : 2 outils formidables**
Aucune introduction nécessaire ici..... Vous êtes déjà convaincus
- **Pourquoi parler de sécurité sur Internet**

La visite de certaines pages Web et la réception ou la mauvaise utilisation de certains courriels indésirables peuvent causer des surprises désagréables, il vaut mieux se renseigner.

Les risques sur Internet pour votre ordinateur.

Les risques sont la destruction de vos fichiers, l'espionnage (par exemple vos mots de passe), l'installation d'un relais sur votre ordinateur à votre insu, les emails indésirables et la déconnexion de votre ordinateur à distance.

La destruction ou l'altération de fichiers se traduit de différentes manières :

- détruire vos fichiers de données (texte, image, musique, vidéo, ...)
- arrêter vos applications en cours d'exécution ou les empêcher de redémarrer
- perturber votre système d'exploitation
- empêcher le redémarrage de votre ordinateur

<http://benefice-net.branchez-vous.com/nouvelles/04-10/08-316503.html> 25 oct. 2004

Sécurité informatique : la plupart des usagers ne seraient pas conscients que leur ordinateur est infecté

Selon une récente étude réalisée pour le compte d'America Online et de la National Cyber Security Alliance, 80% des usagers dont l'ordinateur est infecté par un logiciel espion n'en ont pas conscience. L'étude réalisée auprès de 329 répondants américains chez qui on a inspecté au peigne fin l'ordinateur révèle que près de 3 usagers sur 5 ne connaissent pas la différence entre un anti-virus et un logiciel coupe-feu.

Bien que 85% des gens interrogés disposent d'un logiciel anti-virus sur leur ordinateur, seulement un tiers de ceux-ci déclarent l'avoir mis à jour dans la semaine précédant l'étude.

Au final, le PC d'un usager sondé sur 5 était infecté par un virus alors que 8 sur 10 était l'hôte d'un logiciel espion. La grande majorité des gens dont l'ordinateur était infecté par l'un ou l'autre de ces programmes malicieux n'en avait pas conscience.

Sécurité : les internautes sont beaucoup plus vulnérables qu'ils ne le croient

Selon une étude américaine réalisée par AOL et la NCSA, les internautes se croient en sécurité alors qu'ils sont vulnérables aux infections par des programmes malfaisants ou des logiciels espions.

L'enquête est originale car elle repose sur le questionnement des sujets face à leur sécurité en ligne et fait le parallèle avec la réalité à l'aide du balayage des PC des participants.

L'étude révèle qu'il existe un écart considérable entre le niveau de sécurité informatique effectif des internautes et la perception qu'ils en ont. Ainsi, près des trois quarts (73%) des participants estiment qu'ils sont assez ou très bien protégés contre les virus alors que 15% d'entre eux n'ont pas du tout de logiciel antivirus et que les deux tiers (67%) des sujets ne l'ont pas mis à jour au cours de la semaine précédente.

Pis encore, 63% des participants affirment qu'ils ont déjà été victimes de virus et 19% des PC examinés sont actuellement infectés par un virus, ver informatique ou cheval de Troie.

La situation s'aggrave pour les logiciels espions et publicitaires; pas moins de 80% des PC sondés sont infectés par au moins un module indiscret et 89% des propriétaires de ces ordinateurs déclarent qu'ils en ignoraient la présence. En outre, 90% des sujets dont le PC est «infecté» ne savent pas ce qu'est ou ce que fait un logiciel espion ou publicitaire.

Les choses ne s'améliorent pas beaucoup en ce qui a trait aux logiciels coupe-feu. En effet, deux internautes sur trois (67%) ne possèdent pas de pare-feu, une statistique qui cache toutefois une grande différence entre les utilisateurs munis d'une connexion à faible débit (93%) et à haut débit (49%). Et pourtant, 77% des sujets estiment que leur PC est très bien ou assez bien protégé contre les menaces d'Internet.

Les données du sondage d'AOL et de la NCSA (*National Cyber Security Alliance*) ont été recueillies auprès de 329 internautes adultes entre le 15 septembre et le 8 octobre 2004. La marge d'erreur des pourcentages est de 5,4%, 19 fois sur 20. Tous les détails (en anglais) dans le site StaySafeOnline.info.

.....
<http://www.presence-pc.com/news/La-bataille-sans-fin-de-Microsoft-n5249.html>

Lundi 04 octobre 2004 La bataille sans fin de Microsoft

Le PDG de Microsoft, Steve Ballmer, pense que la lutte pour la sécurité informatique est quoi qu'il advienne une "bataille sans fin".

Toutefois, il ne perd pas espoir dans le combat contre les cyber criminels : "Il y a des gens mauvais dans le cyber espace et ils ne vont pas partir. Nous allons devoir être vigilants." Optimiste, il estime en dépit des alertes de sécurité de plus en plus importantes que la situation s'est grandement améliorée."Ce n'est pas comme il y a cinq ou six ans quand les virus n'existaient pas. Plus de dégâts ont été effectués en d'autres temps par rapport à aujourd'hui. Les douze derniers mois ont été meilleurs en

comparaison des douze précédents. Je veux croire que dans les deux ou trois prochaines années, nous serons assez bon. La sécurité est la base potentielle du commerce. Les gens ont ils assez de foi (en nous) ? C'est la raison pour laquelle nous avons fait de la sécurité un travail prioritaire chez Microsoft."

Pour autant Steve Ballmer n'a pas voulu commenter les rumeurs selon lesquelles Microsoft pourrait développer sa propre gamme de produits de sécurité, mais n'exclut pas celle de futures acquisitions dans ce domaine, tel McAfee. "Nous sommes toujours à la recherche d'acquisitions, mais nous n'avons pas de fonds assigné pour les acquisitions."

Concept d'isolation

L'autre point développé par Steve Ballmer sur le sujet de la sécurité, est celui du concept "d'isolation", qui a déjà été mis à parti avec le Windows XP Service Pack 2. L'idée est de s'assurer que les périphériques et les ordinateurs sont "sains" avant de pouvoir se connecter au réseau. "Dans les entreprises, la première raison pour laquelle les gens attrapent des virus est, en fait, que les machines sont parfois connectées sur le réseau et à d'autres occasions sont en dehors du réseau. Comment vérifier avant que de réintroduire quelqu'un dans le réseau ? C'est une forme d'isolation". Steve Ballmer dit que le but est de maîtriser cette technologie avant la venue de Windows Longhorn.

Ces déclarations ont été faites lors d'une conférence de presse avec les médias britanniques.

- **À qui s'adresse cette capsule**

Cette capsule s'adresse à l'utilisateur qui navigue sur Internet avec son ordinateur et elle a pour but de le sensibiliser aux problèmes de sécurité associés à l'Internet.