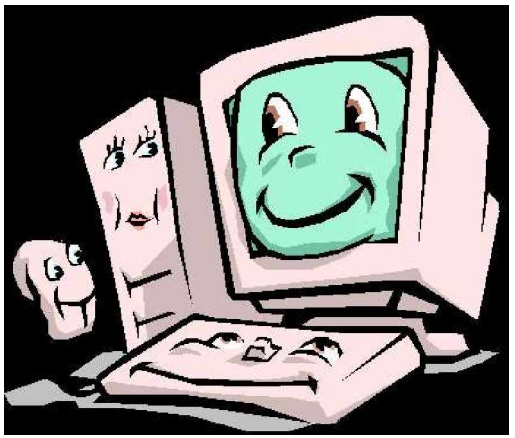
La sécurité sur internet

Ce n'est pas parce qu'il y a des risques d'accident sur la route que nous ne nous déplaçons plus en voiture...

Ce n'est pas parce qu'il y a le sida, que nous ne faisons plus l'amour...

Donc pour l'utilisation d'internet il en est de même : c'est une histoire de conduite et de protection.....



De quoi parle-t-on ?

- **Les fichiers ou programmes malveillants qui posent souci à nos ordinateurs, peuvent se regrouper sous le terme générique de malware. Ils peuvent se classer comme suit :**

Virus	morceau de programme qui se greffe sur un programme, sait se propager sur d'autres programmes
Ver	Code qui utilise les failles des systèmes pour se propager
Mass Mailer	Code qui utilise la messagerie (et ses failles) pour se propager
Trojan	Code qui s'exécute sur la machine cible et permet de communiquer avec l'extérieur.
Spyware	Code qui permet de transmettre les habitudes d'un internaute.
Hoax	Canular ou propagation d'informations erronées
Spam	Envoi de messages non désirés

Un peu de vocabulaire

- **Français ou anglais ...ou les 2**

Virus Ver Trojan	La pas de problème particulier En : worm Fr : cheval de troie
Mass Mailers Hoax Spam	Fr : Logiciel d'envoie en masse de messages électroniques Fr : Message contenant un canulard, rumeur Fr : Multipostage excessif
Spyware Malware Adware Cookie	Fr : Logiciel espion, mouchard, Fr : Logiciel malveillant Fr : Logiciel publicitaire Fr : Fichier témoin, contremarque électronique
Phishing	Fr : Ameçonnage, âppat

Les nuisances

A chacun son rôle !

Virus Vers	Destructions, modification de données, ralentissement, redémarrages intempestifs, modification ou destruction du BIOS et même de la machine (overclocking, fréquences de balayage des moniteurs, …)
Mass Mailers Hoax Spam	Occupation inutile du réseau, propagation de fausses vérités, envoi de publicités non désirées
Trojan Spyware	Récupération d'information confidentielles (mots de passe, certificats, fichiers, N° de cartes bancaires, …) Récupération de la frappe du clavier (Keyloger) Récupération d'habitudes (par exemple sites visités) pour mieux cibler les publicités par le spam Prise de main à distance (Backdoor)
Phishing	Escroquerie par détournement de sites commerciaux

Les virus

Le virus

Le virus est un petit programme exécutable qui a besoin d'un programme plus grand que lui pour se lancer. Son objectif est de nuire. Il peut être fatal aux données enregistrées sur le disque dur.

Les vers

C'est virus autonome qui n'a pas besoin de s'accrocher à un programme pour s'exécuter. Il est capable de s'auto-dupliquer et de s'envoyer sur internet par messagerie par exemple.

Les chevaux de trois

Un programme qui fait croire qu'il a une fonction toute autre que celle qu'il a en réalité. Les noms de fichiers portent souvent à confusion notamment dans les processus windows.

Les virus macros

Une macro est une série de commandes enregistrées, pour automatiser certaines manipulations dans des logiciels comme msword, msexcel. Les macros sont associées à des documents. Les virus sont donc véhiculés par l'échange de fichiers et plus problèmatique de modéles.

Les spywares

- Quels intérêts ?
  - le commerce (publicité, communications téléphoniques jusqu'à 25 $ /min, etc.)
  - le renseignement (espionnage, études, marketing ciblé)
  - Le divertissement
  - Les attaques informatiques

- Quelles formes ?
  - Barres/outils de navigation (Browser Help Object)
  - Outils de redirection (Browser Hijacker)
  - Logiciels de connexion (Dialer)
  - Plaisanteries (Joke)
  - Chevaux de Troie / porte dérobées
  - Outils furtifs d'administration à distance (RAT)
  - Outils de capture d'informations: collecte anonyme de données ou nominative, « datamining ».

D'où viennent-ils ?

- Sites Internet / messagerie / installation de programme
- Failles Microsoft et en particulier Internet Explorer

Le moteur de rendu IE (Trident) est très laxiste et perméable au « mauvais codes » des pages web. Alors que le moteur de Mozilla (Gecko) respecte les standards et les normes, il est donc plus sûr...

- Active X / Java

Petit programme embarqués dans le code des pages web et qui se lancent depuis la mémoire de l'ordinateur.

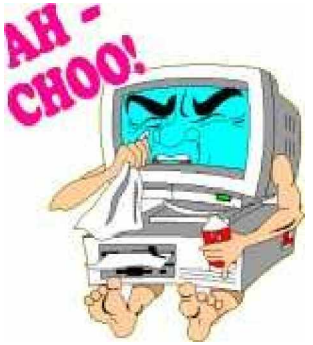
- Installations de logiciels
- Les logiciels de DRM Microsoft / installation de codecs

La DRM permet de défendre techniquement la propriété intellectuelle des images, des textes et des vidéos que l'on diffuse sur Internet.

- Virus

Les symptômes

- Lenteur du PC (CPU)
- Publicités
- Page de démarrage
- Barre d’outils de IE



- Processus de Windows
- Lenteur de l’accès Internet

Le SPAM

Definition

On définit un Spam* comme ***un courrier électronique d'exemplaires identiques, envoyé en nombre de façon automatique, non souhaité, non sollicité, au contenu non désiré, reçu sans le plein consentement du destinataire.***

Autres termes :

Pourriel (Canada), spamming, mail bombing, junk e-mail, junk email, junk mail, scam, script kiddy, script-kiddie, script-kiddies, spammer, spammers, spammeur, spammeurs, unsolicited bulk e-mail

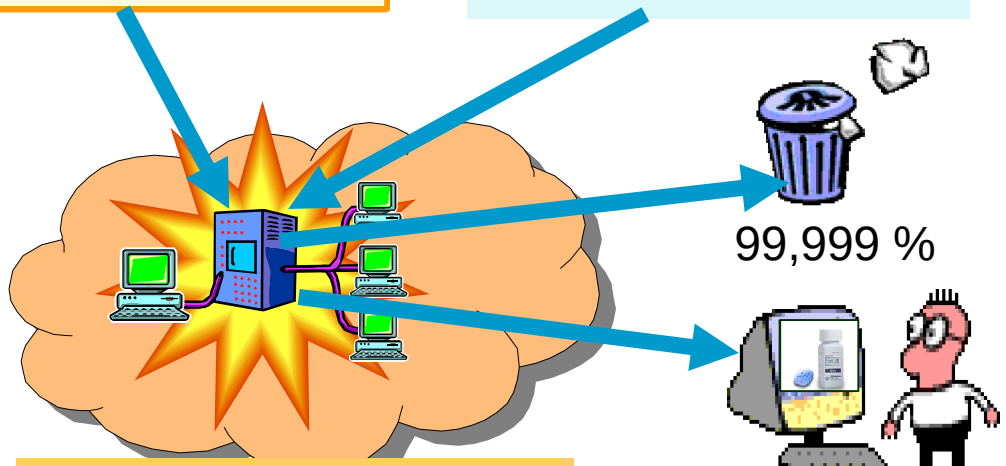
La petite Histoire

A l'origine, SPAM est une marque de corned-beef, et plus précisément un acronyme pour **S**piced **P**ork **A**nd **M**eat (pâté épicé à base de porc et de viandes)

La rentabilité du SPAM

Viagra 100mg
3 tablets 78 $

525 M d'adresses e-mail sur 5 CD set. seulement $99.00



Location de serveurs SMTP

100 $ / 15 M d'emails

99,999 %

0,001 %

Exemple:

Commercialisation de Viagra Prix de vente : 78 $ - marge 18$

Investissement « publicitaire » pour la Diffusion de 15 Millions de spams : **200$**

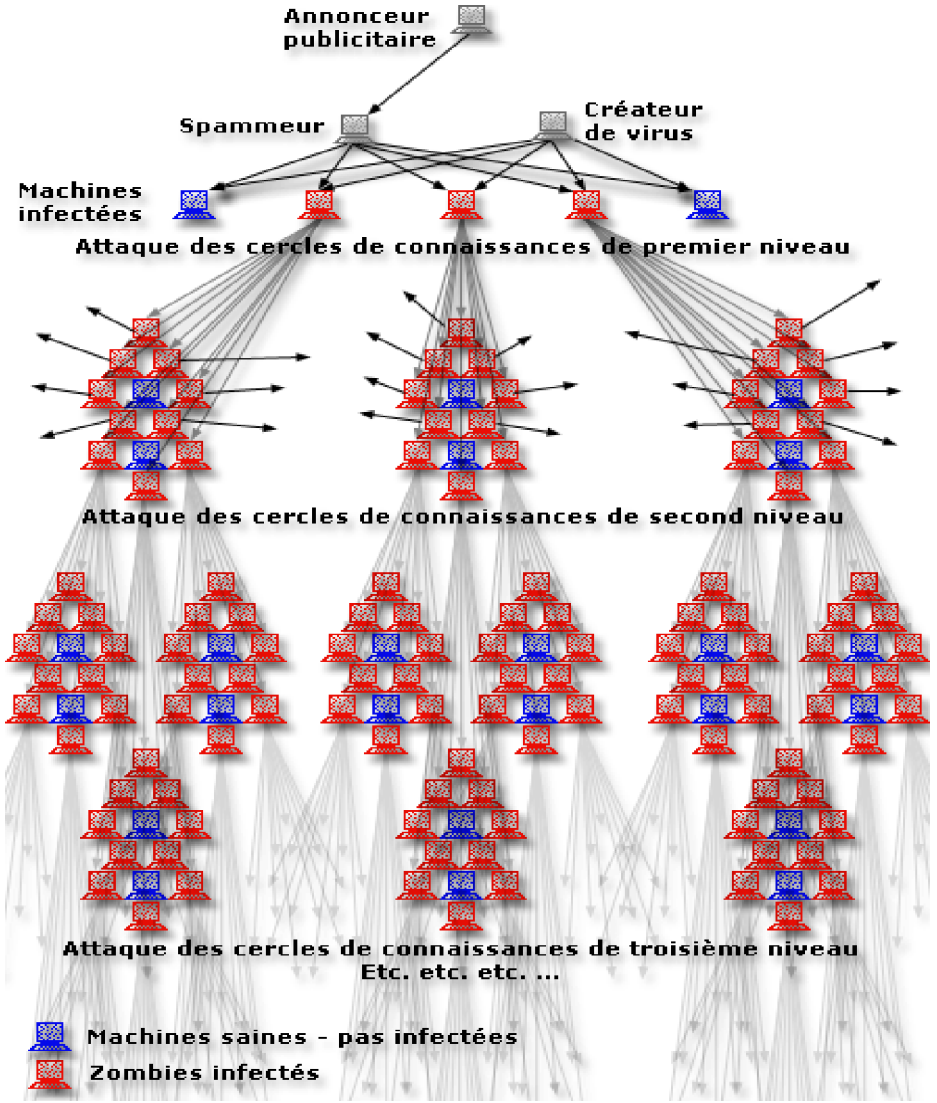
Base de 565 M de courriels valides : **99 $**

Location de serveurs SMTP pour 15 millions de courriels : **100 $**

Retour espéré : 0.001%

Gain= (18$ x 15000) -200$ = **269 800$**

Comment ça marche ?



Un annonceur va utiliser les services d'un « Spammeur » qui avec la complicité d'un créateur de virus.

Le virus installera un mini serveur SMTP et ouvrira une porte dérobée pour un usage ultérieur (Backdoor).

Chaque PC infecté transformé en « Zombie » en utilisant les @ locales est prêt à contaminer le reste de la planète à des vitesses fulgurantes ! (Automatiquement ou sur commande à distance)

Quelques virus : Sobig, Swen, Sober, W32.Gluber.B@mm, MyDoom (Novarg, Mimail), Netsky, Bagle...

Le phishing

Définition

Le phishing c'est la technique employée par **les pirates** et **organisations mafieuses** qui cherchent à tromper l'internaute en l' invitant à rejoindre une adresse détournée affichant la copie d'un écran qui semble légitime (banques, sites d'e-commerces, sites cartes bleues ..) -- Mis en confiance, l'internaute dépose des informations confidentielles comme adresse, mot de passe, coordonnées bancaires, n° de CB …)

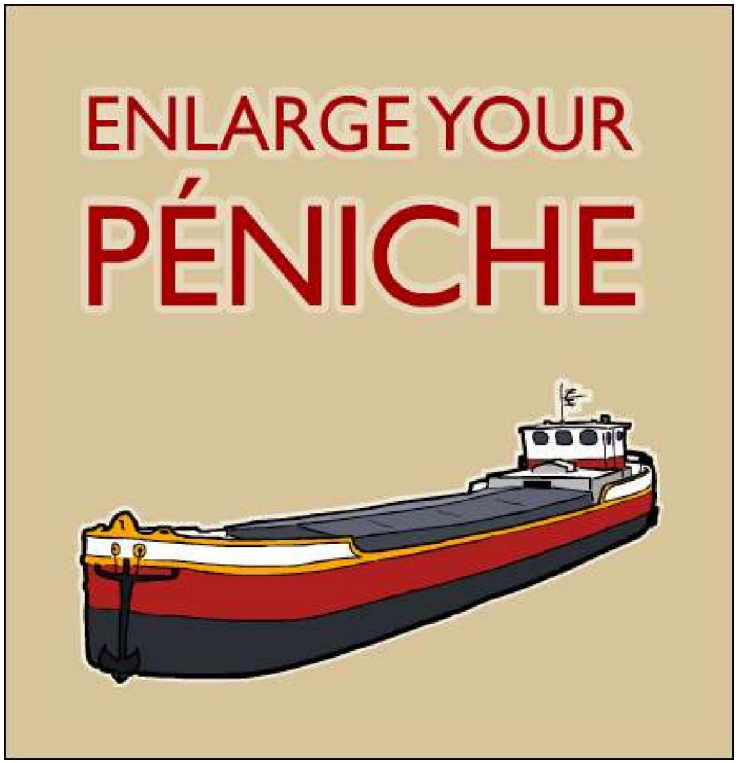
Autres termes :

hameçonnage (Canada), Scam-email

L'origine du terme «**phishing**» pourrait résulter d'une combinaison de «f**ishing**», qui signifie pêcher et de «**ph**reaking,» un mot qui désigne l'accès illégal à un réseau téléphonique

Quelle prévention ?

La meilleure protection pour un ordinateur, c'est d'être éteint !!! ... et encore...



Contre SPAM et spyware

- **Éviter que son PC deviennent un « Zombie »** et complice des spammeurs
  - Anti-Virus à jour
  - PARE-FEU installé (minimum celui de XP-SP2)
  - Système d'exploitation et navigateurs avec les derniers patchs de sécurité (Ex: Windows-Update)
  - Sanner régulièrement son disque avec des logiciels comme Ad-aware, Spybot-Search & Destroy,...

Comportements et attitudes :

- Ne pas répondre au Spam
- Ne pas communiquer son @ de Courriel (forums,IRC , sites douteux, à des inconnus…)
- Ne pas la publier sur les sites Web (Robots de collectes)

Spécial Spam

- Mise en place de Filtres dans les outils de messageries:

Peu efficaces car statiques : les spammeurs ont des outils qui les contournent. IL convient donc d'utiliser un client messagerie avec un filtre évolutif comme celui de **Mozilla Thunderbird,** qui se montre très efficace.

- Exemples de déclinaison du mot « Viagra » :

V agra V0agra V1agra V2agra V3agra V4agra V5agra V6agra V7agra V8agra V9agra Vaagra Vbagra Vcagra Vdagra Veagra Vfagra Vgagra Vhagra Vjagra Vkagra Vlagra Vmagra Vnagra Voagra Vpagra Vqagra Vragra Vsagra Vtagra Vuagra Vvagra Vwagra Vxagra Vyagra Vzagra V&agra Véagra V"agra V'agra V (agra V-agra Vèagra V_agra Vçagra Vàagra V)agra V=agra V^agra V$agra Vùagra V*agra V,agra V;agra V:agra V!agra V?agra V.agra V/agra V§agra V%agra Vµagra V¨agra V£agra V~agra V#agra V {agra V[agra V|agra V`agra V\agra V^agra V@agra V]agra V}agra V<agra V>agra etc. etc. etc

Contre le phishing

le **Forum des droits sur l'internet** (http://www.foruminternet.org/) alerte les internautes sur ce phénomène et leur rappelle les principaux conseils de vigilance à avoir sur l'internet :

- ne jamais communiquer des données sensibles (numéro de carte bancaire, identifiants personnels) en cliquant sur un lien envoyé par courrier électronique ;
- toujours vérifier, dans la barre d'adresse du navigateur, l'adresse du site internet avant de saisir les informations demandées ;
- toujours partir de la page d'accueil d'un site pour accéder aux autres pages, notamment celles où sont demandées des identifiants ;
- lors de la consultation de sites sécurisés (sites bancaires, par exemple), s'assurer de l'activation du cryptage des données (l'adresse du site doit commencer par https et non par http)
- en cas de doute, prendre contact directement avec l'entreprise concernée (votre banque, votre fournisseur d'accès à l'internet, etc.) pour lui signaler le message suspect.

Nos conseils m@ison

- **Ayez un antivirus systématiquement à jour. Pensez également à utiliser le scan de votre antivirus**
- Ayez un parefeu (firewall) actif
- Utilisez un navigateur et logiciel de messagerie sécurisés comme le tandem Firefox – Thunderbird.
- Faites régulièrement les mises à jour de votre système (surtout windows ...) Pour être plus tranquille essayez de passer le pas sous Linux.
- Créez vous une adresse e-mail que vous pourrez laissez trainer sur les sites.
- Utilisez le systéme de paypal pour payer en ligne
- Ne relayez pas n'importe quel message, pétition, ou autre avis de recherche, allez sur le site www.hoaxkiller.com pour vérifier.
- Installez le tandem spybot et ad-aware pour scanner régulièrement votre disque

Nos sources

Pour la réalisation de ce document nous nous sommes aidés des sites suivants :

- http://assiste.free.fr
- http://www.secuser.com
- http://www.clusir-rha.fr
- http://www.hoaxkiller.fr/

Les sites recommandés

- http://www.geckozone.org/
- http://frenchmozilla.sourceforge.net
- http://www.arobase.org/
- http://fr.wikipedia.org (En savoir plus long sur les termes employés)

En savoir plus : Consultez régulièrement le site www.infoweb17.fr