

Le C2I est une épreuve théorique de culture générale informatique (Référentiel C2I). Cours magistrale culture générale info. et sur le vocabulaire d'informatique.

Epreuve théorique : présentation lorsqu'on est prêt (dernier délai mai 2013), pas de convocation -> seul. Examen se passe à la BU. QCM. Pour avoir le C2I il faut réussir l'épreuve théorique. 4 chances, janvier 2012 mai 2012 janvier 2013 mai 2013 mais si on passe en Mai 2013 pas de re-passage. Environ 50 questions. Env. 50 min. Barème qcm : mauvaises réponses ou pas de réponse -1, bonnes réponses +1. Référentiel par compétences (A1 -> B2). Site université extrait du diplôme.

Epreuve pratique -> contrôle continu en TD (8 à 10 séances) des 4 premiers semestres.

Examen terminal d'env. 1h30. Note pour le semestre et pour le C2I.

4 unités étudiées en TD :

- Logiciel de traitement de texte
- Tableur
- Recherche internet
- Elaborer diaporama avec un logiciel de présentation

Pour se présenter à l'épreuve théorique : inscription sur le site internet ENT, onglet C2I, inscription à l'épreuve C2I théorique. Attention pas de convocation alors penser à noter le RDV ! Annulation au plus tard la veille au soir.

Evaluation sur papier en partiel (anticipé probablement). Compte dans l'obtention de l'année universitaire.

Responsable C2I : Yann Morer

Outils bureautique et informatique : C2I

Introduction : outils TIC

A] Définition :

NTI : Nlle technologie de l'information est apparu dans les années 1990. Il est à l'apogée du mariage de l'info, la com et l'audio-visuel. **NTIC → Nlle Techno. de l'info et de la Com.** Nvx mariage de l'info et d'internet. N : Cela va marquer la nlle évolut° techno des produits. Nlle performances au niveau des puces et système transistor, + de fonctionnalité.

B] informations privées et personnelles : obsolescence du matériel :

Multiplicat° des performances du matériel. *Loi de Moore* (ingénieur dans les années 60s) : doublement du nbre de transistor sur une puce, cela aura lieu tous les 24 mois. Dizaine de millions de puces dans les transistors. Cela se mesure sur une échelle nanométrique. Avec cette loi des constructeurs vont améliorer les produits et commercer de nlle gammes de produits. Les matériels nécessite de + en + de performances des logiciels et gourmand au niveau de la mémoire, grâce aux processeurs ainsi que au disque dur et autres cartes (carte mère, carte graphique, carte son...).

C] exemples :

www.c2imes.fr

B7 qu'est-ce qu'un flux RSS ? **

L'utilisation de ces nvx outils vont complètement changer les habitudes nécessitant d'actualiser les connaissances. Mais c'est aussi et avant tout une utilisation pro.

www.internet.gouv.fr

D] les facteurs de l'internet public :

CISI -> Comité Interministérielle pour la Société de l'Informatique. Cela va déf les grdes orientations politique ainsi que les décisions pour prendre la voix de l'intégration et du dvlpmt des nlls technologie. CISI met en œuvre toute les procédures pour l'initiative de critères informatiques. Pas de législation spécifique mondiale concernant internet (prêt logiciel, téléchargement tout genre...). Pas de gendarme internet mondiale possible car pas de règles générales.

Travailler dans un esprit d'ouverture et d'adaptabilité

A] qu'est-ce qu'un logiciel ?

Du point de vue de son utilisation, un logiciel répond à des besoins. **Logiciel : suite d'instructions écrites dans un langage informatique et qui forment un tout cohérent.**

Terminologie créé en 1967 remplace le Soft Wear. Il va permettre à d'autres logiciels de fonctionner et va gérer toutes les autres ressources de l'ordi. L'ensbl des logiciels permettant l'exploitat° de celui-ci se nomme un système d'exploitation.

Pour créer un logiciel il faut utiliser un langage binaire transmissible à l'H. Chiffres utilisés : 0 et 1. Cette traduction va être effectué par un logiciel appelé « compilateur ». Le logiciel dans sa forme compréhensible s'appelle **source du logiciel** ou **source du programme** ou **code source**. La machine peut afficher en langage machine **logiciel binaire** ou le mot **exécutable**.

Logiciel propriétaire : les + nbreux (ils sont distribués sans leur code source pour éviter de pouvoir les comprendre, les dupliquer et donc les graver.). Il peut-ê de type **logiciel Open source**, le code est fournie avec le logiciel. Loi HADOPI 1 : loi française qui a commencé à donner des explications réglementées non applicable lors de la première loi mais lors de la deuxième -> loi HADOPI 2 datant de septembre 2009. **Loi HADOPI 2 « Tout téléchargement intempestif sur un logiciel ou un produit nécessitant l'achat au préalable sera sanctionné par la loi. ». Plateformes illégales existe à cause des pays étrangers pour qui la loi française ne peut pas s'appliquer.** Loi HADOPI 2 renforcée et modifiée par l'intervention de 3 états : brigade internationale créée à cet effet qui va surveiller le territoire français.

1 - La première étape c'est l'envoi d'un mail d'avertissement à la personne grâce à l'adresse IP (3 chiffres avec un point). Les gendarmes vont sur les réseaux où il y a l'ensble des adresses IP. Les gendarmes prennent au hasard des adresses IP et suivent en direct les actions faites sur l'ordi ainsi que l'historique pour voir si ce que l'on fait est légal ou pas. Si pris au piège, l'adresse IP est donnée par le fournisseur d'accès qui fournit plusieurs données.

2 - La seconde étape consiste à surveiller la personne et à la réavertir en cas de récidive. Lettre recommandé avec accusé de réception.

3 - En dernière étape il y a sanction : blocage et coupage de la ligne en écrivant au fournisseur d'accès.

B] la License du logiciel :

Avant d'utiliser le logiciel, on va demander d'accepter la licence existant pour le logiciel. Attention il faut lire l'entièreté de la licence d'un logiciel.

Le droit d'utilisation du logiciel (seulement cercle de la maisonnée).

Le

droit de copie si ce n'est pas stipuler que c'est interdit, c'est autorisé dans le cadre de la maisonnée. Si stipuler, méfait.

Le droit de modification.

Clauses particulières : clauses d'utilisation, de brevet, médicale (épilepsie)...

Toutes ces licences ont une clause de non-responsabilité, de même le fabricant se décharge de toute responsabilité suite à un dysfonctionnement. Limiter le nbre de connexions à distance. Les mises à jour peuvent faire partie d'élmt des licences.

Quels sont les types de licences ?

Les formes de distribution actuelles nous font acheter des produits qu'il ne faut pas confondre avec les logiciels libres → les « free soft ware ». Freeware -> logiciel fourni est gratuit indépendamment de sa licence d'utilisat°. Dans certains cas cela peut-être des logiciels publics. Shareware → logiciel dont l'auteur demande aux utilisateurs une rétribution volontaire (payement).

Un logiciel de domaine public n'est plus soumis aux droits d'auteur, c'est un logiciel libre. Très souvent le code source n'est pas dispo dans ce cas ce n'est donc pas un logiciel libre.

C] les logiciels libres :

Richard Stallman fondateur du logiciel libre et il travaillait dans l'intelligence artificielle. 1983 il a dvlpé un système d'exploitat° libre GNU, le premier mondial. Cela équivaut au système UNIX, licence déposé en 1989 à donner naissance à LINUX. Principe du copie libre où il y a protection légale des 4 libertés fondamentales.

Libertés du logiciel :

Liberté d'exécution, sans limite de temps, de motif, de personnes.

Liberté d'étudier le f°mt du programme et de l'adapter à ces besoins.

Liberté de redistribué des copies.

Améliorer et diffuser les améliorations apportées.

Quel est le coût d'un logiciel libre ? Le logiciel libre vient du mot « free » et du mot « software ». Les logiciels libres vont laisser la libre expression. « freebeer » gratuité, non commercial. Ces logiciels peuvent être dispo pour un usage commercial.

Que-ce qu'un système d'exploitation ?

- Le système d'exploitation majoritaire Société Microsoft, crée par Bill Gates -> Système Microsoft doss. Système Windows avec des formulations progressives et commerciales. Le but de ses sociétés est d'agrandir un parc de logiciel et un parc matériel

- système d'exploitation MacOS réputé pour sa simplicité d'utilisation, avec dernière version MacOSX.

Il y a 10 ans -> 5% des ménages ont des mac. Auj. -> 15%. Prix élevés.

Macintosh a ciblé l'univers professionnel.

- Système d'exploitation Linux : il a ouvert la voie à d'autres produits accessible au grand public, mais tout de même restreint.

Orientation de l'achat d'un client : demande et possession duquel le client aurait besoin. Navigateurs : Internet Explorer, Mozilla Firefox.

Quel suite bureautique le consommateur a-t-il besoin ?

Traitement de texte. Microsoft office (Word traitement de texte, Excel tableur, Access générateur de base de données, diaporama). Open Office. Musique : Windows média Player -> Microsoft.

Logiciel de communication : Skype, Msn, Tweeter, Facebook.

Logiciel professionnel : autocad -> dessin industriel, ciel -> gestion, comptabilité, bureautique -> commerçants -> gestion de caisse.

Logiciel sur les centres d'intérêts de la vie privée : logiciel de jeux, cuisine, généalogie.

D] notion d'interopérabilité :

Notion cruciale : elle va gérer tout ce qui concerne les réseaux téléphoniques mondiaux et internet. Réseau internet : réseau qui va permettre de relier l'information avec une autre personne -> minitel, fibre optique.

Elle veut rendre des réseaux plus homogènes. Cette notion d'interopérabilité s'applique à des milieux diff puisque tout ces secteurs ont besoins de systèmes informatiques et communique entre-elle. Cette notion obéit à des normes clairement établies et univoque. On suppose qu'elle doit être écrite, elle présente des interfaces qui vont poser la cadre du f^omt des réseaux.

Diff entre une norme et un standard : standard désigne ce qui est produit habituellement par un producteur et qui ne dépend que de lui.

Normes : - normes dites ouvertes : publiées, peuvent-être utilisées par tous et librement.

XML . format XHTML ->
internet . format PNG ->
format image . format OGG, VORBIS ->
son - normes avec des approches de

formats dites propriétaires. Le concepteur va utiliser des clés. Elles vont donner accès par une série de chiffres (code d'accès) pour arriver à l'étape suivante. Cela va assurer que l'utilisateur n'utilisera pas un autre logiciel pour lire ces données. Expl : logiciel de messagerie : ICQ, Yahoo, Messenger -> protocole de création normé avec des codes propres, on ne peut pas utiliser les protocoles de messageries pour aller sur d'autres messageries.

E] des normes à distribution restreintes :

Elles sont plus ou moins ouvertes et elles vont assurer la sélection de leurs membres avec un droit d'entrée comme le paiement. Norme vidéo ISO cahier des charges flagrant qui va donner lieu à la création d'une norme segmentée.

Norme ANSI, globalement ces normes vont évaluer la qlté, la valeur et l'analyse d'un produit considéré.

Formats restreints :

- Formats langage java

Formats PDF

algorithme de compression pour rendre la taille d'un fichier moins lourde. Logiciel RAR -> format de compression

- Formats flash

-

-

F] interopérabilité :

On souhaite tous bénéficier de la protection des données : protection à 100% n'est pas garantie en informatique. Hacker ou pirates de l'informatique réseau russe pénètrent les grandes sociétés pour capter leur site internet et au moment où les transactions se font, ils ont tout ce que l'on fait en ligne sur l'écran. Les entreprises ont tendance à renforcer leur système de contrôle avec un accès plus strict et des filtres de plus en plus sévères. Les fabricants de bureautique s'y sont mis. Ils ont créé des systèmes de production drastique et notamment open office ont créé des extensions de fichiers libres. Soit il va devoir forcer l'ouverture du fichier et le voir de manière déformée.

Chapitre 2 : les formats de fichiers ouverts pour l'échange des informations

RGI = Référentiel Générale d'Interopérabilité, logiciel mis à dispositions des administration française dans les choix et au niveau des évolutions de l'ensemble des environnements numériques.

A] le format PNG = Portable Network Graphics :

Formats de fichier graphique ont été développés. Formats ouvert alternatif à un autre format qui est **GIF = Graphics Interchange Format** Pour la compression sans perte, recommandé par la norme internationale ISO.

Norme **JPEG = Joint Photographic Expert Group** défini par l'ISO, tout ce qui est photo. Haut niveau de compression. Mais plus on réduit la compression, plus on perd des infos.

Norme GIF : très répandu, très connu. Créé en 1987, formats propriétaire. On peut faire migrer les fichiers GIF en fichier PNG. La méthode de compression est réversible. GIF ANIME crée en 1989, il va permettre le stockage de plusieurs images dans un même fichier.

FLASH est un format qui permet des réalisations graphique complexes de longue durée. Format propriétaire -> fermé, payant. Société racheté par ADOBE SYSTEME (2005).

B] formats son et vidéos :

MP3 c'est abbreviation d'un format **MPEG = Moving Picture Space Group**. "audio layer free" essai 3 soumis à la norme ISO → MP3. Soumis à la norme ISO grâce à une liscense déposé dans un cahier des charges. Le son reproduit ressemble à une reproduction du son original mais non compressé -> perte significative de qlté sonore.

Chapitre 3 : Intégrer la dimension éthique et le respect de la déontologie

Le droit de l'informatique s'applique et peut être troué par l'internaute, ôtant les gens doivent savoir les règle d'internet

Le droit de l'informatique n'est pas réserver aux juristes mais il doit être compris et assimiler par tous les utilisateurs de l'outil info pour apprendre les règles de bon usage, et les règle de bon usage sont des règles nécessaire car applicable et en vigueur pour tous sur internet

A] Les Droits Fondamentaux De L'Homme Et D'internet

Les droits info ont des rapports conflictuels :

*Le niveau de technologie évolue plus vite que le droit (le droit compense en allant chercher des explications entre chaque mutation technologique)

Logiciel Pire to pire ? (1^{ère} loi = 6 Janvier 1978, c'est la loi informatique des libertés de 7 Janvier 78 et qui constitue un élément fondamental du dispositif législatif concernant l'informatique)

*Le droit de l'informatique est par nature complexe et le législateur sait que les utilisateurs ne font pas toujours la différence entre ce qui est permis et interdit. Le droit info est méconnu et il est finalement peu appliqué au regard des infractions qui sont commises quotidiennement. Cela crédite la thèse key internet possède une zone de non droit et qu'il n'existerait aucune législation qui s'appliquerait au réseau (c'est totalement faux). Il y a de plus en plus d'accord européen transfrontalier

Attention il existe en France au niveau du droit informatique, un code, un ensemble de règles de bon usage en vigueur sur internet. Dans ce code on y apprend des règles de savoir-vivre mais également les règles de lecture, le respect des chartes d'utilisation qui sont en vigueur sur la toile et que tout internaute doit connaître. On peut noter également qu'internet est en même temps un véritable paradoxe sur le plan humain en matière de droit et notamment le droit de l'Homme car il se révèle être très bénéfique en matière de droit de l'homme (il a permis de mettre en avant des situations dont on ne parlait pas, classe sociale, enlèvement etc.) et en même temps l'homme peut bafouer ces droits de l'homme et notamment tout bêtement à bafouer certains droits de la personne privée.

B] Le Droit De L'informatique

On peut depuis 1980 demander au législateur de permettre à quiconque de commettre une infraction et demander une réparation en justice si vous êtes victime d'une infraction

Dans le code pénal il y a un chapitre qui traite des atteintes de traitement automatisé de données.

Dans le 3ème livre il y a 7 articles :

*Le fait d'accéder dans un système, réseaux ou de se maintenir frauduleusement dans tout ou une partie d'un système automatisé : 2 ans d'emprisonnement et de 30 000 € d'amende

Si on modifie le système : 3 ans d'emprisonnement 40 000 € d'amende

Entraver un système, le fausser : 5 ans d'emprisonnement 75 000 € d'amende

*Les personnes physiques coupables dans les délits encourrent également des peines complémentaires : perte des droits civiques (droit de vote), civil et de famille (allocation, RSA) ; Une durée minimum de 5 ans ou plus de ne plus exercer de fonction publique (plus de concours ou une activité professionnelle en rapport avec l'infraction commise) ; confiscation de la chose (logiciel en fonte) fermeture de l'entreprise, exclusion pour 5 ans des marchés publics, interdiction d'émettre des chèques ou de retirer des fonds, toute personne qui aura foulé verra sa peine affichée au grand jour.

Chapitre 4 : Maîtrise de son identité juridique :

C'est quelque chose de fondamentale en info puisque les logiciels sont créés par des développeurs et ces développeurs sont sans limite dans la manière d'exploiter la moindre faille d'un système informatique, évidemment cela veut dire qu'ils

vont pouvoir trouver des idées, mettre au point de nouveau produit, mais cela va donner des idées aux escrocs qui vont mettre au point leur mauvais produit.

Souvent ces logiciels malveillant correspondent à des auteurs de virus qui a une détermination destructrice voir criminelle. Ces createur de virus cherchent souvent une forme de reconnaissance en montrant au monde qu'ils sont intelligent et qu'ils ont su déjouer le système de sécurité

A) L'identité Sur Internet

1) Définition

Par IN (identité numérique) on entend tous les moyens (logiciel ou matériel) qui permettent d'identifier de manière fiable et unique une personne. La plupart du temps l'identité numérique prend la forme d'un couple de donné que sont l'identifiant et le mot de passe. Ces 2 infos vont permettre par exemple d'accéder à un service de web mail, à une espace de travail collaboratif ou tout bêtement à une session informatique. Cette identité numérique pourrai nous faire penser que l'identifiant et le mot de passe créer un anonymat, mais ce n'est pas garanti à 100%, l'anonymat réel n'existe pas sur internet. EN réalité ces éléments d'identité permettent de procéder à une identification cryptographique. La cryptographie c'est le faite de crypter et donc de rendre invisible.

2) Les solutions

- *Il faut utiliser une adresse différant pour chaque activité
- *Utiliser des adresses gratuites lorsque l'on veut surtout être anonyme
- *Limiter les infos que vous transmettre sur internet
- *Évité l'usage de tout ce qui est messagerie de chez Windows, internet exploreur etc.

B) Les Traces Sur Internet

On laisse des traces sur intérêt à chaque passage. Cela veut dire que par le billet du fournisseur d'accès lui-même connecter o ruisseau internet, celui-ci vas vous attribuer un identifiant unique (un adresse IP) cette adresse IP elle est systématiquement enregistrer des qu'il y a activité sur internet, cette adresse IP c'est un couple de donner qui est séparer par des point (ex : 80.10.24.188).

L'adresse IP figure à chaque envoi de courrier électronique.

Une loi oblige tous les fournisseurs d'acer à donner l'ensemble de l'adresse IP et le nom à la police en cas d'affaire

La CNIL public sur son site du conseil et des informations sur la manière de surfer sur le web

1] Les Cookies

Ce sont des fichier qu'un serveur internet peut vouloir stocker sur votre machine afin de mémorisé vos préférences de consultations et ainsi reconnaître la prochaine fois que vous vous connectez a ce site.

Cela serre à reconnaître le visiteur (et donc le différencier) et il va recueillir un certain nombre d'élément :

- *l'adresse IP
- *Recueillir le nom de votre système d'exploitation (Windows, linux etc.) et va reconnaître le navigateur utiliser (ex : internet explorer)

* (le plus important) il garde des infos pratique et statistique comme le nombre de page consultées, ce que vous avez consulté, le nombre de visite total, les actions (genre le cheveu la dauphine etc. le thème quoi) (ça cible les sites marketing) (ex : le cookie permet au serveur de retenir les produit que l'on a placé dans un caddy virtuel et de nous les représenté soit sur le site soit ailleurs)

* la CNIL nous ddt par un communiquer EN 2001 que les cookies jouent le rôle de simples témoin de connexion destiné a facilité la navigation sur un site web ou à en faciliter l'accès et ce sans avoir à Reno tenses identifiant.

Il Ya un texte du 6 janvier 78 qui interdit la collecte de donné opéré par tout moyen déloyale ou illicite.

* Pour ce protéger on peut configurer le navigateur afin de désactiver les cookies, cette désactivation machine vas permettre de limité la propagation de vos informations.

2) Les Espiogiciels (traduction anglaise de Spyware)

Ces spyware prennent une proportion considérable sur le web, c'est un gros Pb pour tout le gouvernement

Un espioiciel c'est un programme qui rassemble des infos à l'insu de son utilisateur et les transmet à une organisation qui cherche à en tirer parti. Et évidemment le but c'est que ces applications puissent être installé sur l'ordinateur du malveillant grâce au navigateur et o système d'exploitations.

Concrètement un spyware peut dresser un profil commercial d'un internat le considérant comme un consommateur en puissance.

Les caractéristiques d'un spyware :

* Toujours furtif

* Il agit sans le consentement de l'utilisateur.

Si c'est furtif mais que l'on vous demande l'accord c'est un adware.

Des fois les Espioiciel vas noyer c'est intention dans les closes

Les degrés de dangerosité :

* il menace la sécurité des systèmes d'information et il faut donc les combattre par tous les moyens. On peut trouver les espioiciel sur internet car ils peuvent être associés à des logiciels proposés en téléchargement gratuit sur internet

A quoi ça sert ?

Ce sont de véritables mouchards électroniques au même titre que les cookies mais qui ont des fonctionnalités encore beaucoup plus étendu.

Ex : Dès l'allumage d'un ordinateur l'espioiciel peut envoyer des données vers un serveur « maitre ».

Il faut éviter de télécharger sur des logiciels en fichier pire to pair, rendre votre anonymat le plus complexe possible

Comment se méfier d'un spyware ?

* Quand vous allumer votre ordi vous voyer que la page d'accueil a était modifié

* Il y a des fenêtres publicitaire qui s'affiche que vous soyez ou non sur internet

* Il y a des barres d'outils qui s'installent toute seule (que vous n'arrivez pas à supprimer)

* Votre ordinateur ralenti de manière inexpliqué

Utilisation de logiciel et de parfum peuvent se révéler utiles parce qu'en effet pour transmettre les données collectées l'espion logiciel utilise obligatoirement une connexion internet.

Certains pare-feu permettront, par exemple à l'utilisateur, d'être alertés des tentatives de connexions à des serveurs distants.

Il a également la possibilité d'utiliser au sein d'un parc informatique d'utiliser un programme info pour se prémunir d'espionnage.

Utilisation de logiciel antivirus et de pare-feu (Firewall) est recommandée. Ils peuvent se révéler utiles parce qu'en effet pour transmettre les données connectées l'espion logiciel utilise obligatoirement une connexion internet. Certains pare-feu permettront, par ex., à l'utilisateur d'être alerté des tentatives de connexions à des serveurs distants. Il y a également la possibilité d'utiliser au sein d'un parc informatique, des programmes spécifiques pour se prémunir contre les espions logiciels.

Ex. de **spyware** : téléchargement de musique sur casa, téléchargement programme p2p. Spyware est le plus gros pourvoyeur d'ennui informatique il peut voir ce que l'on fait, prendre des données. Logiciel anti-spyware -> **cydoor**. En fonction des données (infos transmises par l'utilisateur) on va avoir des bannières publicitaires qui vont être téléchargées sur le disque dur et vont être affichées régulièrement quand le programme casa est exécuté. Le logiciel va protéger les éléments nominatifs. Le logiciel cydoor coûte de plus en plus cher : entre 2000€ et 5000€. Il est reconnu par la **Commission National Informatique et Liberté (CNIL)** et qui va capter et filtrer les données personnelles ensemble des éléments d'un ordi à caractère nominatif ne peut être prélevé sans déclaration au préalable.

Trend micro -> logiciel antivirus. Propose une base de données de virus. Oppose des black door -> carte noire.

D] les traces sur logiciel :

La CNIL qui régule les flux internet mettait en garde que l'info n'était pas facile, non transparente et non maîtrisée par l'utilisateur. Permet de dire que cette conception est bien naïve.

1] les outils :

On peut activer sur le PC des mouchards permettant l'accélération de la traçabilité. Les sociétés nécessitant sécurité l'utilisent.

- au niveau de la **messagerie** : pour les courriers envoyés et afin d'éviter que tout soit stocké dans « éléments envoyés », il faut juste désactiver la case à cocher « copier les messages envoyés » dans « éléments envoyés ». On peut également activer l'onglet envoi dans la commande, outils -> option -> onglet envoi de la commande. Même si on désactive on ne voit plus les éléments visiblement, mais l'informaticien peut avec des programmes.

- dans **office** on stocke **tout type de documents**, on peut enregistrer avec « enregistrer sous ». Onglet outils -> option de sécurité -> activé onglet supprimé les infos personnels.

- **TWEAK** permet d'effacer systématiquement les traces une fois qu'on a fini d'utiliser le PC : fin de chaque jour, demi-journée, heure.

- onglet **paranoïa** : option permet d'effacer toutes traces internet.

- **Windows** crée des empreintes par une page Ethernet qui aura un numéro de 48 bits conçu pour être unique. Article dans le « New-York Times » critique Windows -> scandale de publier des infos face au respect de la vie privée.

Chapitre 5 : sécurisation des informations sensibles

Les dangers d'internet

1] Les virus et les macrovirus

Définitions :

Virus : c'est un **programme** qui effectue certaines actions et en général cherche à se reproduire. Le but est de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecter. But ? -> se répandre à travers tous les moyens d'échanges de données numériques.

Programme : instruction écrite dans un langage de programmation.

Un petit million de virus circulent dans le monde avec un danger bien réel. Eviter de propager aux autres.

Macrovirus : s'attaque aux macros présents dans nos logiciels grâce au procédé VBA de Microsoft -> système plus sensible et malléable pour les virus

Vers : se répand dans les courriers électronique en profitant des failles des logiciels de messagerie. Dès qu'ils ont affecté un ordinateur il envoi eux-mêmes dans tout le carnet d'adresse ce qui fait que l'on va recevoir le virus dans le message d'une personne connu. Expl : I Love You.

2] les HOAX : canulars

Canulars -> expl de la rumeur d'Orléans (vole de fille dans les cabines d'essayage de magasins). **Fausse infos ou une rumeur**. La plupart du temps cela se véhicule sous la forme d'un **spam** se basant sur le courrier électronique.

Un forwarder fait relayeur virus. C'est la base du système.

Est-ce que un HOAX est dangereux ? Il n'est pas aussi dangereux que d'autre virus car il ne met pas en défaut la sécurité.

Effets pervers :

- Engorge réseau et boîte aux lettres
- Sert à la désinformation en faisant circuler de fausses infos ou des rumeurs non-fondées et cela décrédibilise le moyen de diffusion que représente internet.

www.foaxbuster.com

Comment éviter :

- option alerte dans messagerie
- ne jamais entrer dans une chaîne de solidarité
- Arrêtons d'être tous crédules.

4] les chevaux de Troie

Histoire mythologie grec.

Point de vue informatique : programme qui effectue une tâche spécifique à l'insu de l'utilisateur.

Un cheval de Troie ne se reproduit pas mais il peut être intégré à d'autres virus. Sachant que les virus peuvent se reproduire, dans ce cas le cheval de Troie aussi. Il est toujours exécuté de manière furtive. Il peut être exécuté dès le démarrage de l'ordinateur. Il est programmé par exécution automatique.

Sur quel support peut se cacher un cheval de Troie ?

- Un logiciel qui lui servira d'hôte.
- Un autre virus
- On doit faire attention sur internet, expl en téléchargement de jeu, il se peut qu'un cheval de Troie furtif se cache à l'intérieur des éléments de téléchargement. On peut transmettre des infos de notre clavier.

Le cheval de Troie stocke les infos.

5] les portes dérobées : back door

Permet à un programme d'accéder à distance à un ordinateur.

C'est en fait un cheval de Troie distant => back door. C'est une prise de contrôle à distance. Souvent utilisé lors de contrôle dans le cadre de la maintenance.

Principe : dérober sans le consentement du propriétaire.

2 types de fonctionnement :

- **la partie client**

- **la partie serveur.** Composant serveur : sur la machine de la victime grâce à un virus ou un cheval de Troie. Récupéré le mémoire de tout ce qui aura été fait. Le composant serveur ouvre un port réseau une fois que tout a été mis en place. Va faire en sorte que l'utilisateur malveillant puisse se connecter en toute tranquillité. Une fois cela fait il pourra réaliser toute une série d'action.

Expl d'action :

- transférer des fichiers dans les 2 sens. Expl : Changer la monnaie.

-

Supprimer et modifier les fichiers informatiques -> vol d'informations.

- Prendre

tous les Enregistrements et saisis du clavier

- Enlever anti-

virus.

- Couper notre

serveur pour permettre à d'autres attaquants de se connecter à notre machine.

6] le PHISHING :

Vient de la pêche (Fish en anglais)

Technique d'ingénierie sociale qui va envoyer un courriel qui se fait passer pour une organisation avec laquelle on est en relation.

Dans le courriel on va nous demander de remplir des renseignements personnels. Intention généralement est de pirater le compte bancaire.

A pour but de faire capture d'écran, capture de logo, police de caractère, mise en page : tout ce qui fait vrai de ce que l'on veut copier.

