Université de Limoges

Se protéger des dangers d'Internet

xavier.montagutelli@unilim.fr
Service Commun Informatique
Responsable de la Sécurité des Systèmes d'Informations
Université de Limoges

Version du 25/01/2012

Université de Limoges

Plan

- Avant-propos
- Qu'est-ce que « Internet » ?
- Internet et droit
- Les logiciels malveillants
- Le courrier électronique
- Le web
- Autres usages (P2P, jeux, réseaux sociaux, …)

Avant-propos

- Horaires : 9H-12H30, 13H30-16H30
- Fiche d'évaluation à remplir à la fin
- Avertissement
  - Pas de « recette miracle » dans cette formation
  - Orienté système Windows
  - Pas une formation sur Windows, ni sur un logiciel particulier
- **Objectif** : donner des clés de compréhension, sur Internet, sur les menaces, pour comprendre et s'adapter
- Posez des questions au fur et à mesure

Avant-propos – Vous

- Tour de salle
- Vos attentes : quels « dangers » ? Pour la maison ou le travail ?

Université de Limoges

De quoi va t'on parler ?

- Internet :
  - Le réseau « extérieur », public
  - Beaucoup de ressources, et des « dangers »
- Quels dangers ?
  - Arnaques, escroqueries : argent, manipulation
  - « Chats » sur Internet : créer des rencontres « pour de vraies » ...
  - Détournement d'identité : argent, pénétrer sur d'autres systèmes, réputation
  - Prise de contrôle de votre machine par un pirate : créer une machine « esclave »
  - Vol des données professionnelles ?
  - Autres ?

Université de Limoges

De quoi va t'on parler ? Les vulnérabilités

- Une *menace* exploite une *vulnérabilité*
- Chez vous
  - Humaines : crédulité, curiosité, appât du gain, luxure, …
  - Logicielles : failles de votre système (Windows, Mac OS, …) ou des logiciels utilisés
- Chez vos « partenaires ». Exemple : si un site marchand où vous avez laissé votre numéro de CB se fait pirater ?)
- Sur l'infrastructure d'Internet

↳ Nous allons surtout prévenir ou réduire les risques en travaillant sur les vulnérabilités

↳ Autres solutions : élimination (pas d'Internet), acceptation (tant pis), transfert

Université de Limoges

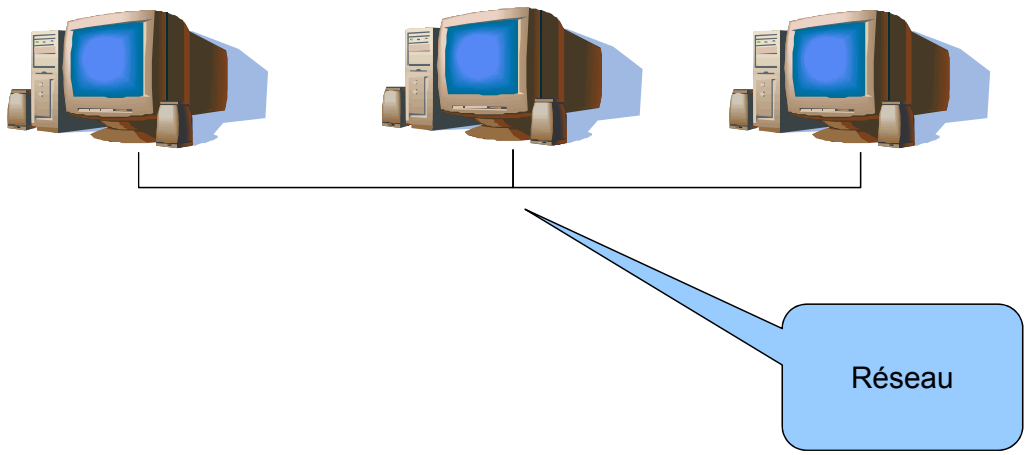
Plan

- Avant-propos
- Qu'est-ce que « Internet » ?
- Internet et droit
- Les logiciels malveillants
- Le courrier électronique
- Le web
- Autres usages (P2P, jeux, réseaux sociaux, …)

Université de Limoges

Internet – Réseau

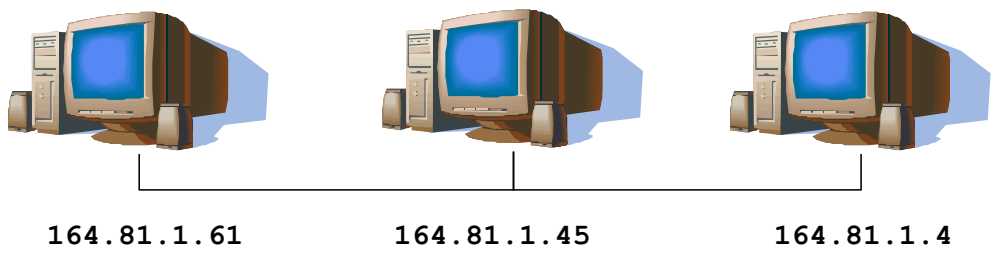
- Un *réseau informatique* est un ensemble d'ordinateurs reliés entre eux et qui peuvent échanger des informations



Université de Limoges

Internet – Réseau, adresse IP

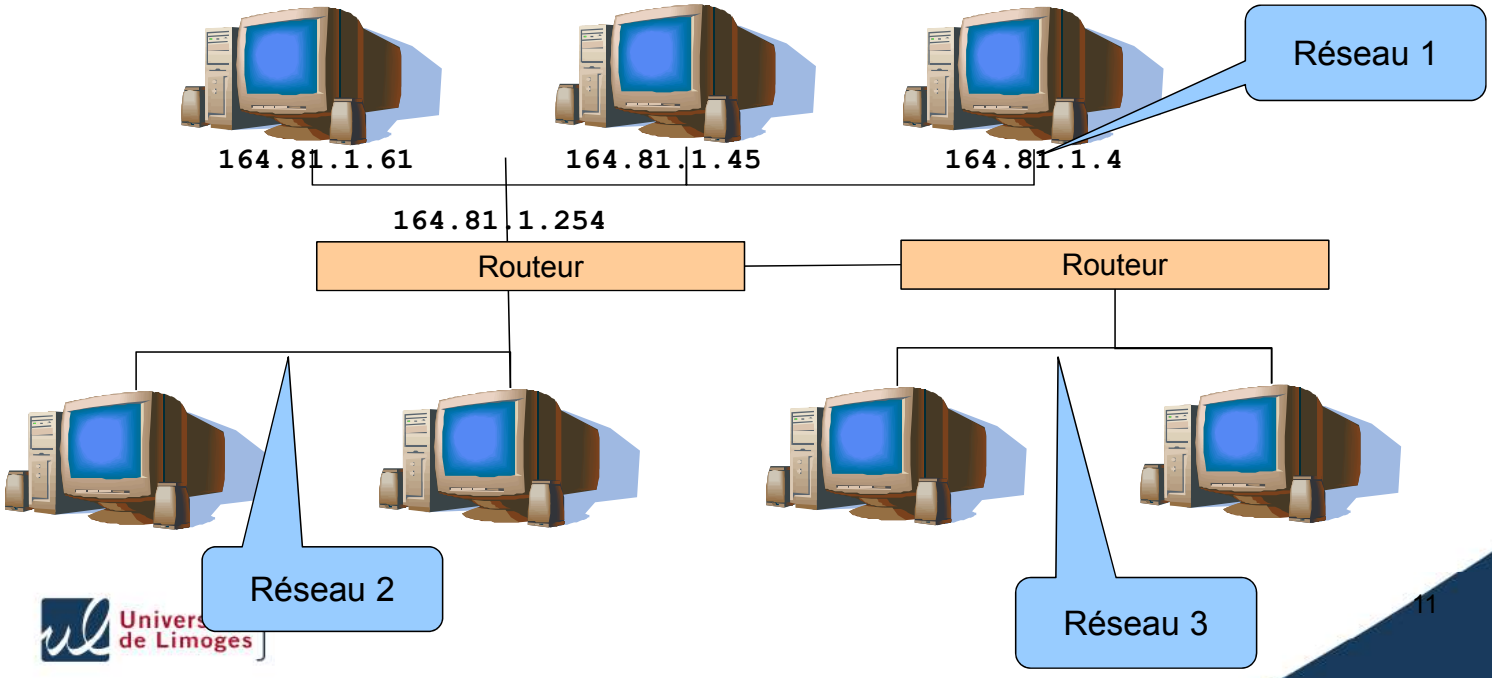
- L'adresse IP (*internet protocol*) identifie une machine sur le réseau
  - Elle est unique
  - Elle permet la communication d'une machine à une autre.
- Exemple : 164.81.1.61



Université de Limoges

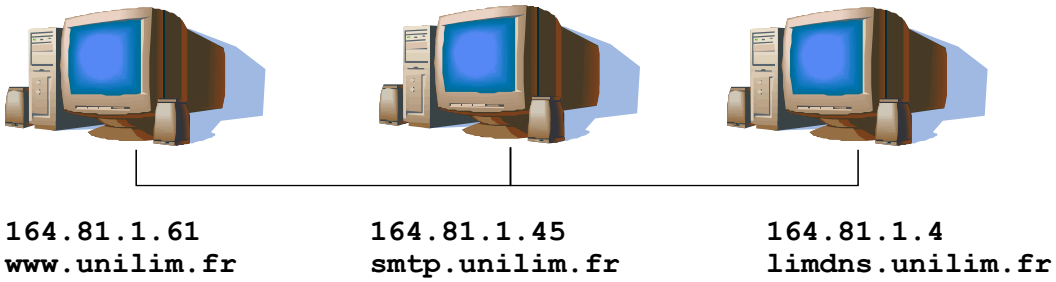
Internet – Réseau (2)

- Un *routeur* (*passerelle*, *gateway*) est un élément du réseau qui permet de passer d'un réseau à un autre

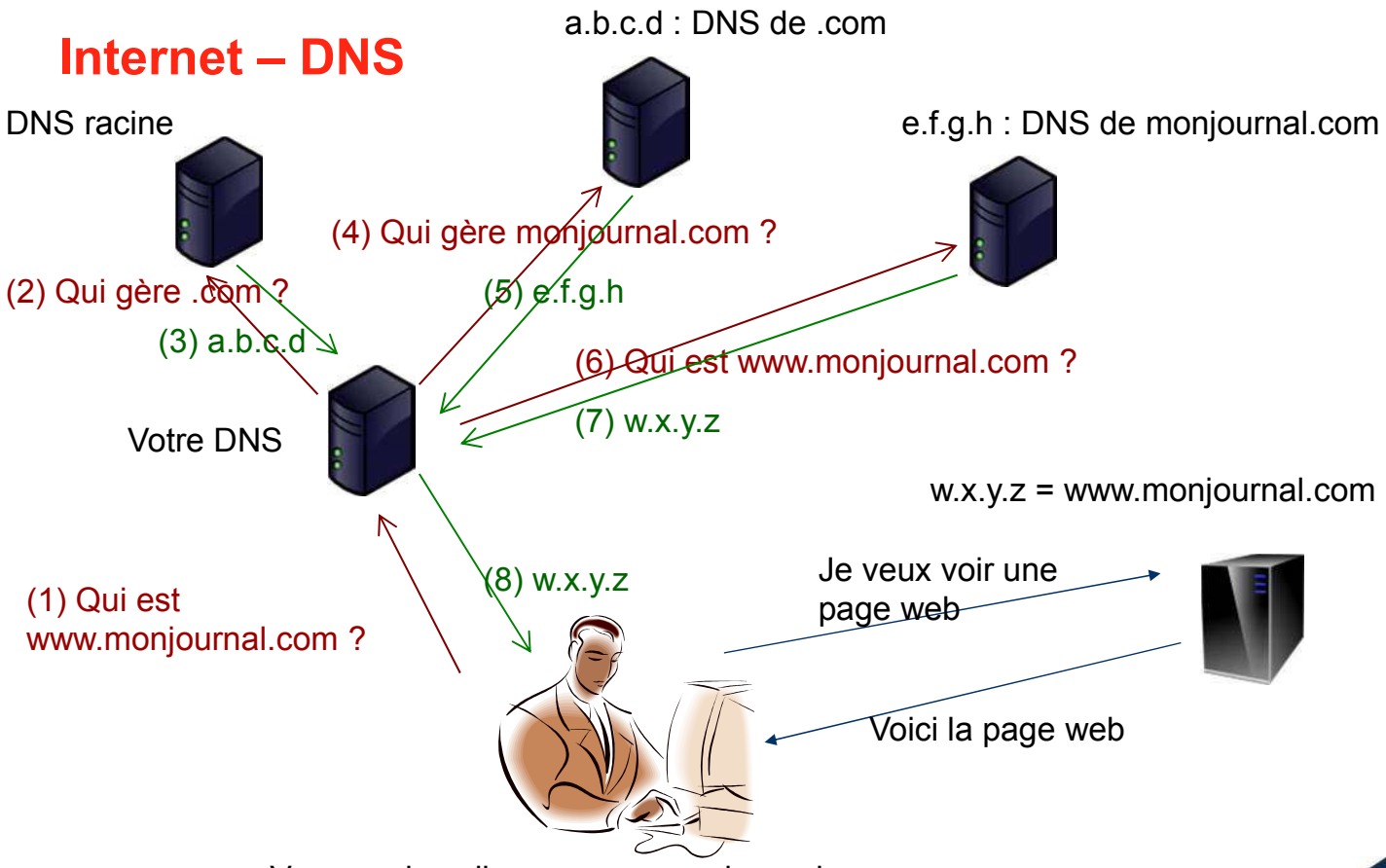


Internet – Adresse et nom DNS

- Un nom plutôt qu'une adresse : www.unilim.fr
- L'équivalence entre les deux est faite par le « DNS » (*Domain Name Service*) et les serveurs de noms



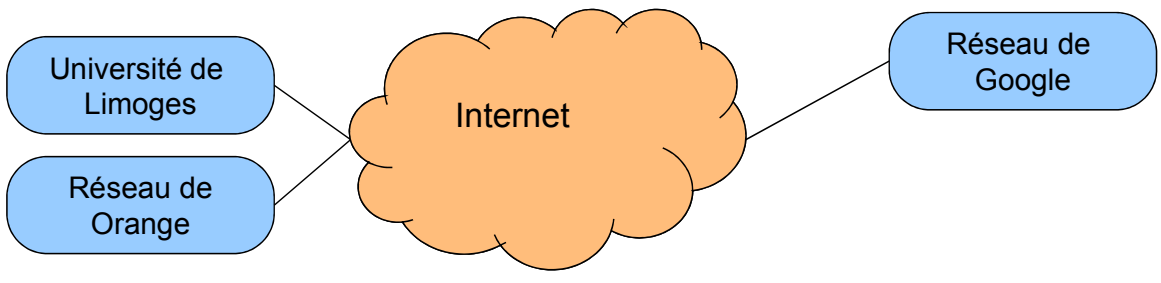
Internet – DNS



Université de Limoges

Internet – Origines (1)

- « Internet » est un réseau mondial, public. C'est le « réseau de réseaux », qui regroupe des millions de réseaux (par exemple celui de l'université de Limoges)
- Basé sur des travaux de l'armée américaine (*Defense Advanced Research Projects Agency*), lancé en 1958 suite au lancement du satellite Russe Spoutnik (autre projet connu : le GPS !)



Université de Limoges

Internet – Origines (2)

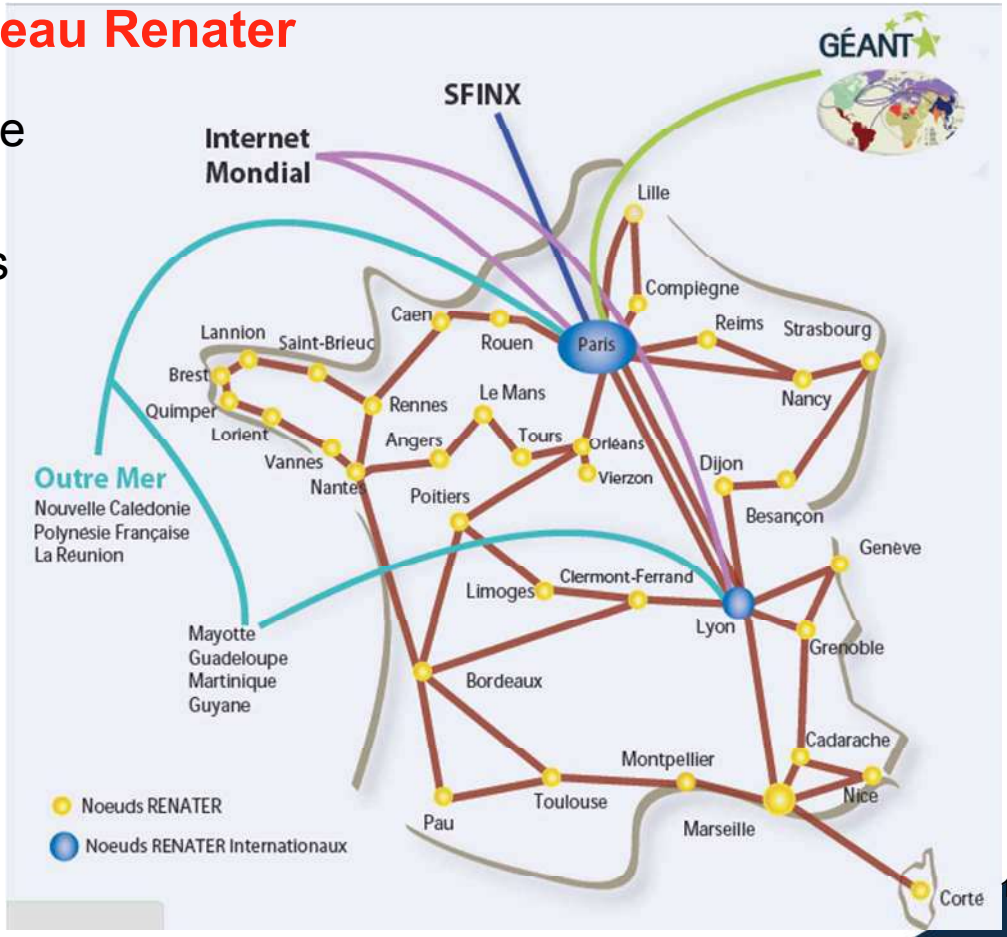
- Premier réseau « TCP/IP » dans une université américaine, en 1983
- Une application « ancestrale » : le courrier électronique. Débute en 1965.
- Début 1990 : le web apparaît, créé au CERN (*Organisation européenne pour la recherche nucléaire*). Le web est basé sur HTTP (comment échanger des données) et HTML (langage qui décrit un document du web)
- Toutes les normes et langages sont publics. Ils ont été discutés et amendés par toute une communauté. Ils ne sont pas la propriété intellectuelle d'une entreprise privée !

Internet – Réseau Renater

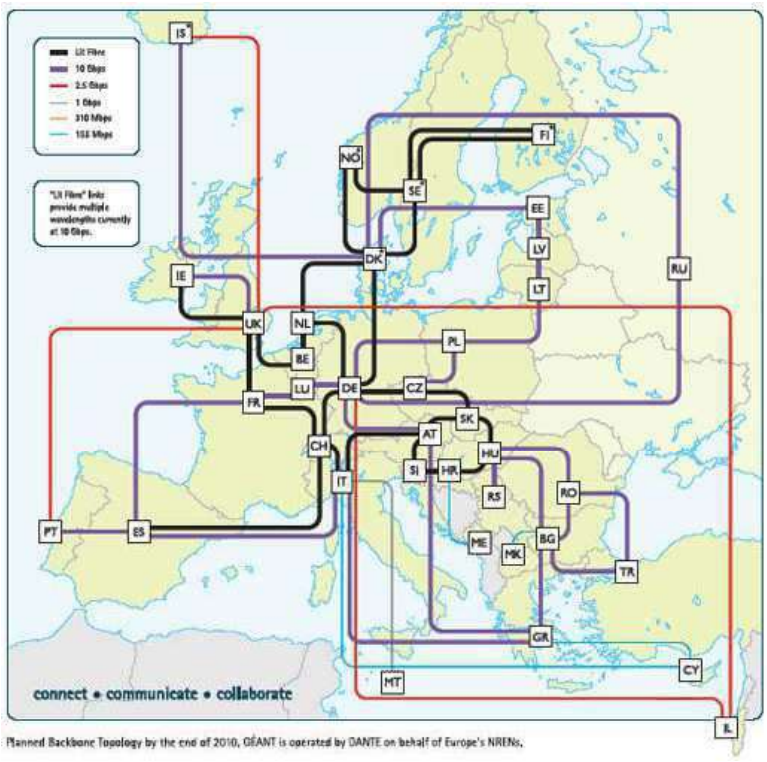
- *Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche*
- Forme juridique : un GIP
- 800 sites reliés en France
- Une équipe dédiée à la sécurité : le CERT-Renater
- Une charte d'utilisation :
  - Pour l'éducation et la recherche
  - Rappel : les usagers doivent respecter la loi
  - Utilisation personnelle autorisée si la consommation de ressources est modérée

Internet – Réseau Renater

- Réseau France
- Liaisons internationales



Internet – Réseau européen GEANT



Planned Backbone Topology by the end of 2010, GÉANT is operated by DANTE on behalf of Europe's NRENs.

Plan

- Avant-propos
- Qu'est-ce que « Internet » ?
- Internet et droit
- Les logiciels malveillants
- Le courrier électronique
- Le web
- Le P2P

Internet et législation

- Réponse juridique simple : ce n'est pas une zone de non-droit, le droit habituel, établi, s'applique
- Il y a des législations spécifiques
- Une jurisprudence qui se construit
- L'aspect trans-frontalier rend en pratique compliqué les actions judiciaires ...
- Exemple : la justice française se reconnaît compétente dès lors qu'un site est orienté vers le public français (arrêt cour de cassation 9 sept. 2008)

Internet et législation – Propriété intellectuelle

- Code de la propriété intellectuelle (CPI) : concerne les logiciels (assimilé à une oeuvre littéraire ou artistique), pas seulement les musiques, films, etc.
- Renforcé par la loi « DADVSI » (*droits d'auteurs et droits voisins dans la société de l'information*) du 1er août 2006. Nouvelles infractions : contournement de mesures techniques de protection, mise à disposition de logiciel permettant d'accéder à des œuvres protégées, ...
- Au pénal, peine encourue : 300 000 € d'amende, 3 ans de prison ; au civil, réparation du préjudice
- Mai 2007 : le Conseil d'Etat annule une décision de la CNIL, la « chasse aux pirates » par des logiciels automatiques est rendue possible ...

Université de Limoges

Internet et législation – Propriété intellectuelle (2)

- Loi « HADOPI » ou « Création et Internet » (Loi n°200 9-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet) : pour protéger les droits d'auteur
- Création de l'HADOPI, autorité administrative indépendante
  - Surveillance de l'Internet par les ayant-droits
  - HADOPI reçoit les saisines des ayant-droits et commence une « riposte graduée »: courriel, puis recommandé, puis coupure accès Internet après transmission au parquet
  - Labellisation de sites de téléchargements légaux
- Débuts effectifs octobre 2010

Université de Limoges

Internet et législation – Injure et diffamation

- Injure et diffamation publiques, contre un particulier (même s'il n'est pas nommé, mais s'il est identifiable) : 12000 € d'amende (loi de 1881)
- Injure et diffamation publiques, contre une personne ou un groupe de personnes, à raison de leur race, ethnie, religion, sexe, handicap : 1 an d'emprisonnement, 45000 € (loi de 1881)
- Injure et diffamation non publiques (exemple : dans un échange privé) sont aussi punissables (moins lourdement)
- Plainte : par la personne diffamée ou injuriée. Ou le ministère publique s'il y a discrimination

Internet et législation – Vie privée

- Le respect de la vie privée est garanti par de multiples textes
- Loi « Informatique, Fichiers et Libertés », 1978, modifiée en 2004
  - Le traitement automatisé de données à caractère personnel doit être déclaré à la CNIL (*Commission Nationale de l'Informatique et des Libertés*, autorité administrative indépendante)
  - Le responsable des traitement a des obligations : informations, consentement, confidentialité
- « Espionner » une personne (enregistrer ses paroles, ses images à son insu, dans un cadre privé) : 1 an, 45000 €
- Interception, détournement de télécommunication (de mauvaise foi) est aussi répréhensible

Internet et législation – Vie privée (2)

- Le courrier électronique constitue une correspondance privée (Cour de Cassation, 2 oct. 2001)
- Mais ... dernières jurisprudences : au travail, le courrier ou les données sont réputées professionnelles, sauf si elles indiquent leur caractère privé (classé dans un dossier « Personnel » ou « Privé » par exemple)
  Arrêt « CATHNET-SCIENCE », Cour de cassation Chambre sociale 17 mai 2005
  Arrêt « DATACEP », Chambre sociale de la Cour de cassation mai 2007

Université de Limoges

Internet et législation – Langue française

- L'emploi du français et obligatoire pour les personnes publiques
- Loi Toubon de 1994
- Circulaire de 1999 sur les sites Internet pour les établissement publics de l'Etat
- Une liste des termes français pour l'informatique : délégation générale à la langue française (http://www.culture.fr/culture/dglf)
- Exemples : courriel

Université de Limoges

Internet et législation – Les mineurs

- Des protections spécifiques
- Pornographie enfantine : offre ou diffusion, 3 ans d'emprisonnement et 45000 € d'amendes ; détention, 2 ans et 3000 €
- Loi sur la confiance en l'économie numérique (LCEN, 2004)
  - Les fournisseurs d'accès à Internet doivent informer leurs abonnés et proposer des mesures techniques pour protéger l'accès à certains services. Ils doivent concourir à la protection.
  - **Obligation de dénoncer** les activités illicites constatées !
  - Les hébergeurs ont l'obligation de réagir promptement si on leur signale un contenu illicite
- Lopssi 2 : l'autorité administrative peut désigner aux FAI des adresses ou sites à bloquer. Début du filtrage d'Internet, sans jugement.

Internet et législation – Accès aux systèmes

- Loi Godfrain 1988
- Punit le fait de pénétrer dans un système informatique sans autorisation (frauduleusement), de modifier des données, ...
- Devrait s'appliquer à tous les programmes de type « virus », aux pirates, etc.

Internet et législation – Au travail

- L'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps du travail (Cour de Cassation, 1991)
- Dans le respect des lois et règlements (ex: ne doit pas concerner la vie privée)
- Si c'est justifié
- Si nominatif : le déclarer à la CNIL
- Doit en informer ses employés
- Ces règles sont souvent présentées dans une « charte » informatique, assimilée à un règlement intérieur

Plan

- Avant-propos
- Qu'est-ce que « Internet » ?
- Internet et droit
- Les logiciels malveillants
- Le courrier électronique
- Le web
- Autres usages (P2P, jeux, réseaux sociaux, …)

Logiciel malveillant – Description

- Autres appellations : pourriciel, *malware*
- Diverses catégories : *virus, ver, spyware*, *adware*, *keylogger*
- Plus subtils / intéressés que les virus des années 90
- Dangers multiples :
  - Gêne : affiche des pubs, ralentit ou plante la machine car mal conçu
  - Espionnage : mot de passe, code d'accès aux sites bancaires, documents envoyés au pirate
  - Contrôle la machine : votre PC devient un *zombie*, contrôlé par le pirate à votre insu, et enrôlé dans un *botnet* (*robot network*)
- Qui ? Des sociétés commerciales, des pirates isolés, des mafias

Logiciel malveillant – Comment s'installe-t'il ?

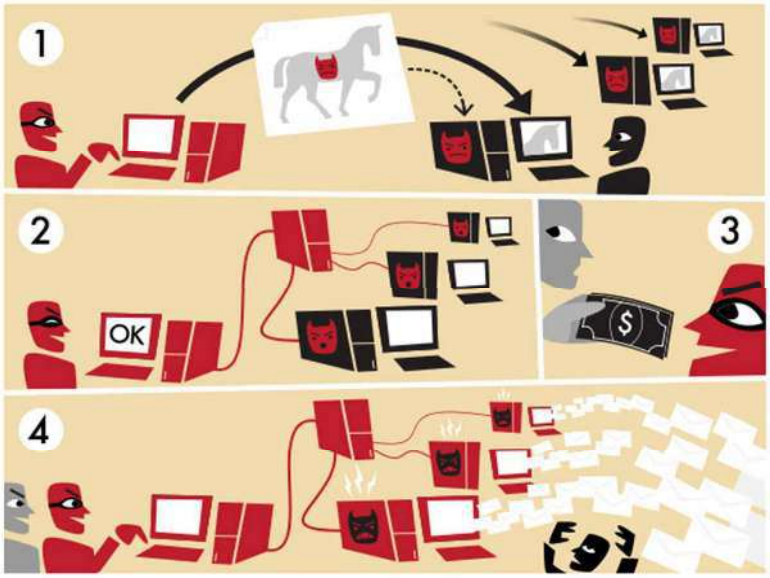
- Vous ouvrez la porte :
  - Parce qu'il se « déguise » (cheval de Troie)
  - Par curiosité et puis il s'incruste (vous cliquez sur un lien dans un courriel …)
- Il force la porte en utilisant une faille logicielle (du système, d'un autre logiciel)

Logiciel malveillant – Cheval de Troie

- Comme Ulysse avec le cheval de Troie, un logiciel malveillant est parfois caché dans un autre logiciel qui parait sans danger et attrayant ...
- Exemples types : économiseur d'écran (avec des chats, avec des blondes pulpeuses), jeux d'argent, faux antivirus
- Le Troyen peut être envoyé par mail, directement ou sous forme de lien. Il peut être vanté dans des forums sur le web. Il est parfois inclus dans des CD distribués par des magazines informatiques !

Logiciel malveillant – Botnet

- Premier *botnet* dangereux en 2002
- Une tendance lourde, touchant beaucoup les ordinateurs du grand public



« How a botnet works », par Tom-B (Wikipedia)

Logiciel malveillant – Exemples de botnets

- Deux pirates hollandais arrêtés suite à une enquête du FBI. 100 000 PC contrôlés http://www.informaticien.be/news_item-5547-Deux_pirates_hollandais_avec_un_botnet_de_100_000_machines_arretes.html
- Un californien contrôlait 600 000 PC, 100 000 $ de gains, 3 ans de prison
  http://www.zdnet.fr/actualites/internet/0,39020774,39363062,00.htm
- L'Espagne démantèle le plus vaste réseau de PC fantômes « Plus de 13 millions de machines dans le monde étaient contrôlées à l'insu de leurs propriétaires par trois Espagnols. Des grandes entreprises étaient aussi infiltrées. »
  http://www.lefigaro.fr/sciences-technologies/2010/03/03/01030-20100303ARTFIG00759-l-espagne-demantele-le-plus-vaste-reseau-de-pc-fantomes-.php

Logiciel malveillant – Fondamentaux pour les éviter

- Comment faites-vous pour éviter d'avoir un accident de voiture ?
  - Entretien du véhicule, contrôle technique
  - Conduite prudente : en respectant les règles, en s'adaptant
  - En utilisant des équipements de sécurité : ceinture, airbag
- Idem en informatique
  - Une entretien à faire
  - Des bonnes pratiques faciles à suivre ... et qui peuvent éviter beaucoup d'ennuis

Fondamentaux – Les mises à jour

- Les mises à jours (*updates*) sont des correctifs logiciels
- Pour améliorer, ou plus important, pour corriger des bogues (*bugs*), c-à-d des erreurs dans le logiciel
- C'est la visite d'entretien de la voiture !

Pourquoi faire les mises à jours ?

- Les pirates, les virus profitent de ces failles pour infecter votre machine
- L'exploitation peut se faire en navigant sur un site web, en ouvrant un courriel, un document (Word, PowerPoint, PDF, un fichier de musique, …)
- Règle : ne pas être « Has been » !

Fondamentaux – Mises à jour Microsoft

- L'éditeur Microsoft propose depuis Windows 2000 des mises à jour automatique (*Microsoft Update*)
- Permet de mettre à jour Windows, Office, Outlook
- Menu `Démarrer` → `Panneau de configuration`, puis `Mises à jour automatiques`
- Règle : mises à jour en mode automatique
- Durée du support :
  - 10 ans pour les correctifs sécurité sur les produits « entreprise »
  - XP Edition familiale SP3 sera aussi supporté 10 ans (2014)
- A l'université : le SCI propose un outil aux administrateurs de parc informatique pour faciliter ces déploiements

Fondamentaux – Windows et Service Pack

- Microsoft propose des améliorations et corrections dans un gros « paquet », nommé *Service Pack* (SP en abrégé)
- Vérifier sa version : menu `Démarrer` → clic droit sur `Poste de travail`
- Pour Windows XP, le SP 3 (sorti printemps 2008) est **obligatoire**
  - Apporte le firewall et améliore beaucoup d'éléments en sécurité
  - Les versions antérieures ne reçoivent plus les correctifs de sécurité !
  - Pour XP : le SP 2 n'est plus supporté depuis juillet 2010
- Pour Vista : SP2 obligatoire (mai 2009), les versions avec SP1 ne seront plus supportées à partir de juillet 2011
- Pour Seven : SP1 (février 2011)

Fondamentaux – Windows et Service Pack (2)

- Pour installer un SP sous Windows, lancer Internet Explorer et aller sur http://update.microsoft.com : le site devrait vous le proposer s'il n'est pas installé
- Centre Microsoft : http://windows.microsoft.com/fr-FR/windows/downloads/service-packs
- Le SP3 de XP si vous voulez le transporter chez vous :

  http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=5b33b5a8-5e76-401f-be08-1e1555d4f3d4

Fondamentaux – Mises à jour des autres logiciels

- Il faut aussi faire les mises à jour des autres logiciels : les pirates sont **très** imaginatifs !
- Produits Mozilla (Thunderbird, Firefox) :
  - `?` → `Rechercher des mises à jour ...`
  - MAJ automatisées : `Outils` → `Options`, partie `Avancé`, onglet `Mises à jour`
- Adobe Reader : `?` → `Rechercher les mises à jour ...`
- Quicktime : `Aide` → `Mise à jour ...`
- Adobe Flash Player : aller sur le site http://www.adobe.com/products/flash/about/

Université de Limoges

Fondamentaux – Mises à jour MS Office

- Pour savoir la version utilisée : http://office.microsoft.com/fr-fr/word-help/quelle-est-la-version-doffice-que-jutilise-HA101873769.aspx
- Comme pour Windows : installer les Services Packs et les mises à jours de sécurité
  - Office XP : SP3 – Ne reçoit plus de mises à jours depuis juillet 2011
  - Office 2007 : SP3 – Support jusqu'à avril 2014
  - Office 2010 : SP1
- Faire les mises à jour : avec Microsoft Update

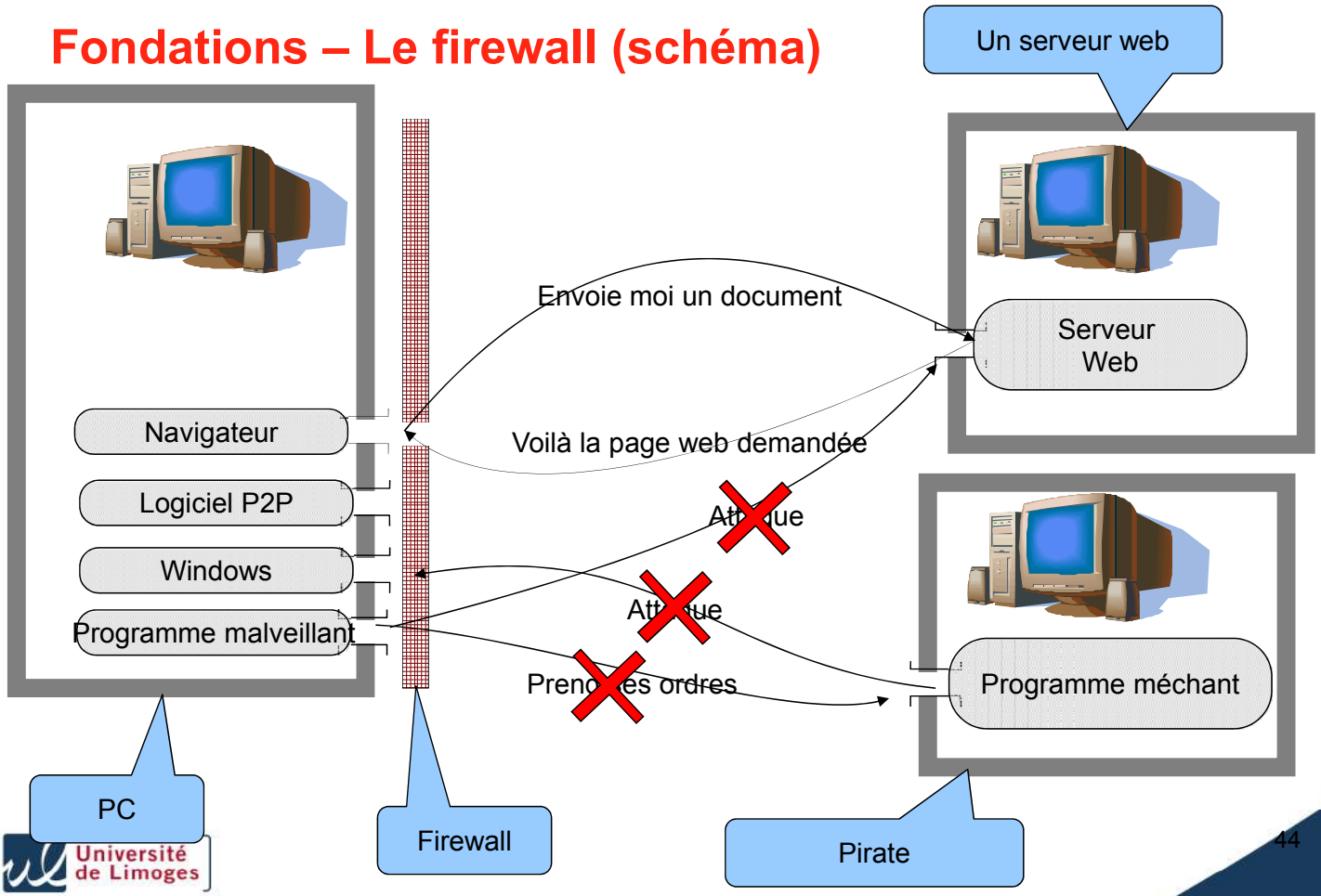
Université de Limoges

Fondamentaux – Le firewall

- Les ordinateurs communiquent entre eux en échangeant des messages
- A travers des portes, identifiées par un numéro
- Chaque programme ouvre une porte différente
- Le pare-feu (garde-barrière, *firewall*) bloque les portes, ou contrôle leur accès
- Il ne débloquera que ce qu'il faut (en théorie)
- Il est conseillé d'utiliser cette « ligne Maginot »

Université de Limoges

Fondations – Le firewall (schéma)



Université de Limoges

Fondamentaux – Antivirus

- Un antivirus est un programme contre les virus :-)
- Mode « temps réel » (ou analyse à l'accès) : il analyse les fichiers à chaque fois qu'on lit ou écrit sur le disque
- Mode « scan » : vous lui dites de vérifier le contenu de votre disque dur
- D'autres fonctions (suite intégrée) : protection contre les spywares, firewall, contre les spams, etc.
- Nécessite des *signatures* à jour (faire une vérification quotidienne)
- Ce n'est pas la solution à tout : toujours en retard, parfois aveugle

Fondamentaux – Quel antivirus à l'université ?

- Des marchés signés par le Ministère existent
- Contrat en cours avec l'éditeur Symantec (*Norton Antivirus*) + Kaspersky + McAfee
- Installation : par votre informaticien de composante
- A déclarer au SCI

Fondamentaux – Quel antivirus chez vous ?

- Des antivirus gratuits (pour usage *personnel*) :
  - Avira : Antivir Personal
  - Avast! Free Antivirus
  - AVG Anti-Virus Free Edition
  - Comodo
  - Microsoft Security Essentials
- Pas d'antispyware, pas de protection du mail, pas de pare-feu
- Beaucoup d'antivirus payants (souvent sous forme d'abonnement), avec une offre plus large que le seul AV (type *Internet Security*). Cher ?
- Une offre existe souvent chez les FAI (Offre *Antivirus Firewall* chez Orange, *Pack Sécurité* chez Neuf, *McAfee Internet Security* chez Free, tous à 5€/mois)

Fondamentaux – Antivirus « Live »

- Des AV « live », par le web
  - On va sur le site d'un éditeur d'antivirus
  - On accepte un composant logiciel
  - On peut ensuite scanner un fichier ou le disque complet
- Pratique pour faire une double vérification avec son anti-virus local
- Exemples :
  - http://www.bitdefender.fr/scanner/online/free.html
  - http://www.f-secure.com/fr_FR/security/security-lab/tools-and-services/online-scanner/
  - http://housecall.trendmicro.com/fr/
  - http://security.symantec.com/sscv6/WelcomePage.asp
  - http://onecare.live.com/site/fr-FR/default.htm (Microsoft)

Fondamentaux – Antispyware

- Espiogiciel : recueille des informations personnelles et les envoie au concepteur ou à un tiers, sans autorisation explicite et éclairée de l'utilisateur
- Certains sont intégrés à des logiciels « normaux » : lire les conditions d'usage ?
- Logiciel de protection « spécifique » : Adaware, Spybot Search and Destroy, Windows Defender de Microsoft (inclus dans Vista et Seven)
- « Alourdi » encore la machine s'il est mis en temps réel
- Parfois utile en cas de doute ?

➥ Comme les antivirus, protections souvent inefficaces

➥ Exercez votre esprit critique avant tout

Logiciel malveillant – Signes d'infection

- Une alerte de l'antivirus – Parfois <u>après</u> l'infection !
  - ☞ Se méfier des faux antivirus !
- Vous ouvrez un document (provenant d'un courriel, d'Internet) et l'application « plante »
  - ☞Evitez de transmettre le document à vos voisins de bureau pour voir si eux arrivent à le lire …
- Votre machine devient « instable »
- L'antivirus ne marche plus ou n'arrive plus à faire ses mises à jour

Logiciel malveillant – Nettoyage – Solutions classiques

- ☞ Problème : on n'est jamais sur de ce qu'on fait quand un PC démarre sur un disque avec un virus ou n'importe quel logiciel malveillant
- ☞ Solutions classiques :
- Démarrer Windows en mode « sans échec » (*safe mode* en anglais) et lancer votre anti-virus
  - Appuyer sur F8 au démarrage
- Utiliser plusieurs antivirus, par exemple avec ceux par le web
- Utiliser des outils de « nettoyage » (outil dédié, antivirus, antispyware)
  - Trend Micro Damage Cleanup Engine http://fr.trendmicro.com/fr/products/enterprise/damage-cleanup-services/
  - Kaspersky Removal Tools http://www.kaspersky.com/virusscanner
  - Microsoft Safety Scanner http://www.microsoft.com/security/scanner/fr-fr/default.aspx

Logiciel malveillant – Nettoyage – Solutions poussées

- Ré-installer votre système
  - ☹ Pas facile
- Débrancher le disque dur, le mettre comme disque secondaire sur une autre machine pour l'analyser. L'analyse sera ainsi faite depuis un système « sain »
  - ☹ Il faut avoir deux machines, pouvoir débrancher le disque
- Démarrer la machine sur un CD *de boot* qui contient un antivirus
  - BitDefender Rescue CD http://www.bitdefender.com/support/How-to-create-a-Bitdefender-Rescue-CD-627.html
  - Kaspersky Rescue Disk http://support.kaspersky.com/faq/?qid=208282173
  - F-Secure Rescue CD http://www.f-secure.com/en_EMEA/security/tools/rescue-cd/
  - Avira AntiVir Rescue System http://www.avira.com/en/support-download-avira-antivir-rescue-system

Fondamentaux – Utiliser un compte limité / séparé

- Sous Windows XP/Vista/Seven, plusieurs types de compte avec des *privilèges* différents
- Un compte *normal* ne pourra pas installer de logiciel : seul un *administrateur* pourra le faire
- Empêche un utilisateur de l'ordinateur de faire une bêtise, volontairement ou non (s'il télécharge un virus, celui-ci ne pourra pas s'installer)
- Chaque compte a ses fichiers, son environnement
- Utilisation type au boulot / à la maison
  - L'informaticien de votre site est le seul *Administrateur*
  - Vos enfants utilisent un compte normal, les parents sont Administrateurs

Fondamentaux – Utiliser un compte limité / séparé (2)

- Avec les versions *Vista* et *Seven*, Windows diminue les droits des comptes « Administrateur »
- Il vous demande une autorisation pour récupérer les droits complets
- Ne pas cliquer automatiquement « oui » quand il demande une élévation des privilèges !

Fondamentaux – Utiliser un logiciel alternatif

- Les pirates qui utilisent les vulnérabilités logicielles ciblent les plate-formes les plus communes
- Conséquence : moins d'attaque sur les logiciels « alternatifs »
- PDF : pour remplacer Adobe Reader (calamité en terme de sécurité)
  - SumatraPDF : très léger, rapide http://blog.kowalczyk.info/software/sumatrapdf/free-pdf-reader.html
  - PDFXChange Viewer : très puissant http://www.tracker-software.com/product/pdf-xchange-viewer
- Bureautique : OpenOffice
- Navigateur web : Firefox, Chrome
- Système : Mac OS, Linux au lieu de Windows ?

Université de Limoges

Fondamentaux - Les clés USB

- Sous Windows, les clés USB servent de vecteur à des virus (une clé portant le virus, connectée à un PC, l'infectera)
- Windows peut déclencher automatiquement l'exécution d'un programme, sans aucune action ni confirmation de votre part : très dangereux !
- Pour se protéger : utiliser les mesures de protection http://www.unilim.fr/sci/article94.html
- Depuis février 2011, Microsoft propose une mise à jour de niveau *Important* qui désactive l'autorun des clés USB http://support.microsoft.com/kb/971029

Université de Limoges

Fondamentaux – Logiciels « de confiance »

- Installation d'un logiciel : vous lui accordez « les pleins pouvoirs »
- Ne pas installer un logiciel provenant d'une source « non sûre »
  - Préférer le téléchargement depuis le site de l'éditeur
  - Se méfier des « petits utilitaires » vantés sur des forums

Université de Limoges

Plan

- Avant-propos
- Qu'est-ce que « Internet » ?
- Internet et droit
- Les logiciels malveillants
- Le courrier électronique
- Le web
- Autres usages (P2P, jeux, réseaux sociaux, …)

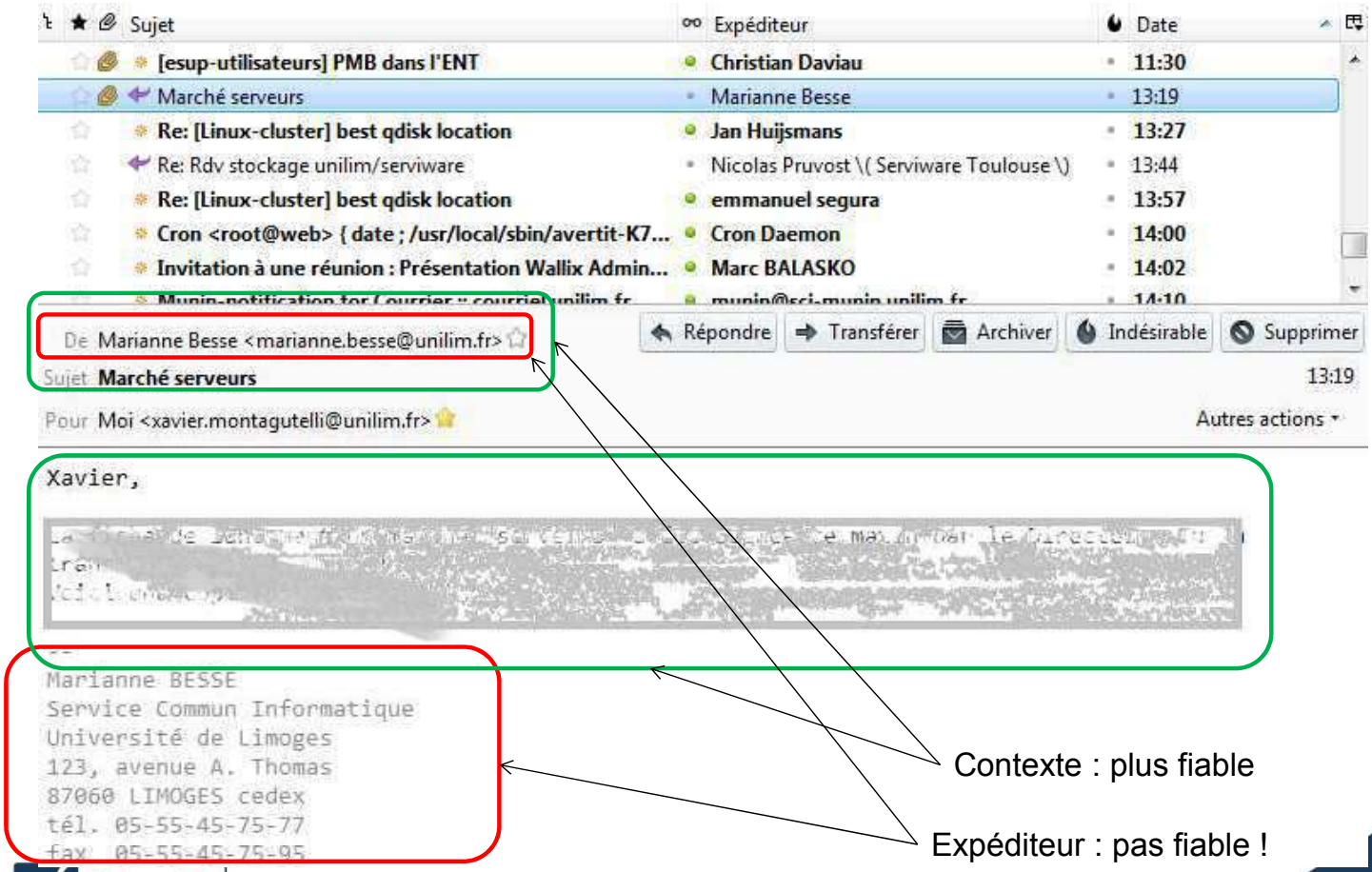
Université de Limoges

Le courrier électronique

- Courriel, *electronic mail*, *e-mail*
- Adresse mél :
  - xavier.montagutelli@gmail.com
  - svp-ent@unilim.fr
- Environ 200 milliards de courriels échangés chaque jour dans le monde
- A l'université : 120000 courriels échangés chaque jour, pics à 250000 (~ 10 Go de données)

Courriel – Origine d'un message

- Comment savoir qui vous écrit ?
- L'adresse d'expéditeur :
  - N'est pas contrôlée, il ne faut jamais s'y fier aveuglément
  - Identique à l'encart situé habituellement en haut à gauche dans un courrier papier indiquant l'expéditeur
- Le contexte, les éléments évoqués, sont en général les seuls moyens de vérifier l'identité de l'expéditeur



Courriel – Protéger ses échanges

- Deux mesures de protection des courriels :
  - Signature
  - Chiffrement
- Signature : prouve l'identité de l'expéditeur **et** la non modification du contenu du message (intégrité)
- Chiffrement : seul le destinataire peut déchiffrer (confidentialité)
- Moyens techniques : avec PGP ou avec S/MIME (des certificats)
- Le particulier va plutôt utiliser PGP, un organisme va plutôt utiliser des certificats (exemple : le CNRS)

Courriel – Spam

- Publipostage électronique
- Massif (plusieurs milliers ou millions de destinataires)
- Souvent répété
- Non sollicité !
- Collecte préalable d'adresse mél : par des fichiers de clientèle, par collecte automatique sur le Web, etc.
- Dans le monde, plus de 100 **milliards** de spams **par jour** !
- 80 % des courriels en Amérique du Nord
- A l'université, réception de 20000 spams / jour

Courriel – Spam, bonnes pratiques

- Règles générales :
  - Ne pas répondre aux spams
  - Ne pas cliquer sur les liens
  - Mieux : ne pas les ouvrir !
- Sites respectueux de la loi : proposent un lien de désabonnement. Exercer son jugement (si on a confiance dans le site émetteur) !
- A l'université : tous les messages sont « notés ». Si spam, ajoute `{Spam?}` au début du sujet
- Autres solutions : utiliser les filtres antispam du client de messagerie

Courriel – Notes sur le paramétrage de Thunderbird

- Menu Outils → Paramètres des comptes
  - Paramètres serveur → Bouton Avancés… : décocher « Afficher uniquement les dossiers avec abonnement »
  - Paramètres des indésirables
    1) cocher « Activer les contrôles adaptatifs … »
    2) cocher « Se fier aux entêtes … de : SpamAssassin »
    3) Cocher « Déplacer les nouveaux courriels indésirables vers » : « Autres » et choisir la boîte « Spam » sur IMAP
- Menu Outils → Options
  - Partie Sécurité, onglet Indésirables
    1) Cocher « Quand je marque des messages comme indésirables » : « les déplacer dans le dossier Indésirables »
    2) Cocher « Activer la journalisation des indésirables »
  - Partie Sécurité, onglet Courrier frauduleux : cocher « Signaler si … frauduleux »
- Menu Affichage → Dossiers : choisir « Tous »

Université de Limoges

Courriel – Eviter le spam

- Inscription sur des sites Internet : ne pas cocher la case « J'accepte de recevoir des offres de la société XXX et de ses partenaires »
- Utiliser des adresses mél « jetables », par exemple en créant des *alias* de votre messagerie principale :
  - Possible à laposte.net (Mes préférences -> Créer et supprimer mes alias), hotmail, yahoo, …
  - Adresses « + » chez gmail (xavier.montagutelli+laredoute@gmail.com)

Université de Limoges

Courriel – Vecteur de virus

- Les virus se transportent parfois à travers des courriels (et les pièces jointes)
- A l'université, un anti-virus analyse chaque message et le bloque si un virus est détecté
- Mais parfois, ça passe quand même !

Courriel – Canular

- Canular (*hoax*) plus ou moins anodins ...
- « La petite Lili a disparue. Aidez-nous ! Voilà sa photo »
- « Si vous avez tel fichier sur votre ordi, effacez-le, c'est un virus. Transmettez l'information à vos amis ! »
- Appels à la haine, au racisme ...
- Désinformation, manipulation de l'opinion (faux courriels islamistes)
- Effet « boule de neige »
- Pour vérifier : http://www.hoaxbuster.com

Courriel – Attrape-nigaud

- Spam « nigérian » : « je suis la fille de feu M. Xxxx, que Dieu soit avec vous, aidez-moi à récupérer mon argent »
- Pleins de variantes (« ancien soldat en Irak »)
- Promettent en général de l'argent facile ...
- Si vous suivez la « procédure » : vous serez volé

Université de Limoges

Courriel – Hameçonnage

- Aussi appelé filoutage, *phishing*
- Attrape-nigaud évolué : par imitation d'un site « de confiance », ou par crédulité, les pirates obtiennent des informations confidentielles (numéro de carte bleue, identifiant et mot de passe)
- Exemple : appel à don après le Tsunami au Japon
- Exemple (merci à Olivier Krempt, FDSE, pour l'exemple qui suit)
  - un courriel semble provenir des Impôts (ou d'un site qui a votre numéro de carte bleue : e-bay, …)
  - Vous cliquez sur un lien web …
  - … et vous visitez un site qui n'est pas le vrai

Université de Limoges

Subject: SFR Groupe:Erreur de prélèvement sur votre dernière facture
From: service@sfr.fr
Date: Thu, 5 Jan 2012 23:23:39 -0500

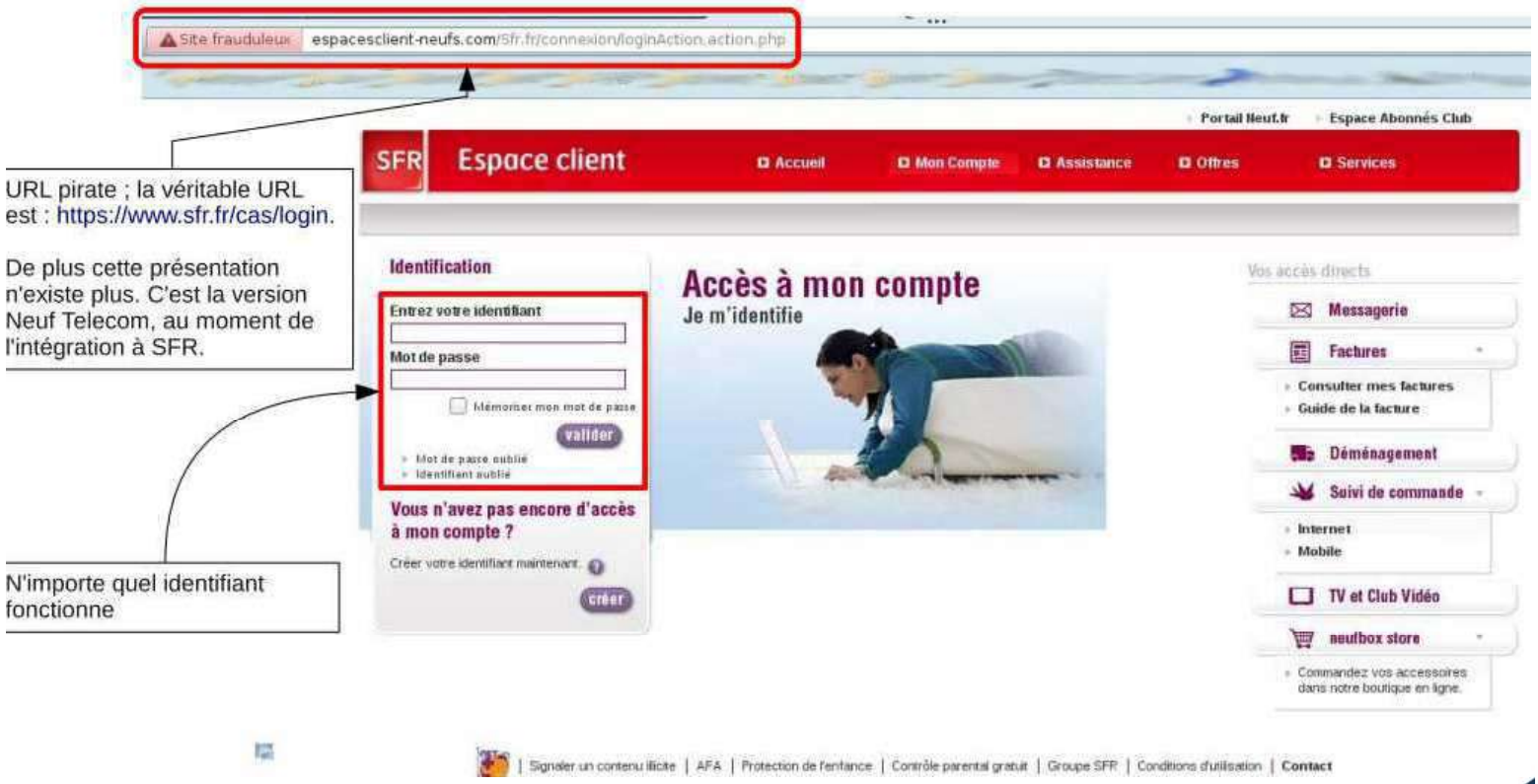
Chèr(e)s client(e)s
Votre prélèvement bancaire a éte réfusé par votre banque.
Afin de régulariser votre situation veuillez vous referez ci-dessous.
Lors de l'echec de la régularisation de votre facture.
nous procéderons à la suspension de votre ligne téléphonique, cette intervention vous sera facturé
nous vous prions de bien vouloir cliquer sur le lien ci-dessous et fournir toute information susceptible d accelerer le réglement de votre impayer.
Remplissez le formulaire de paiement en cliquant sur le lien suivant:
Connectez-vous Cliquez Ici

Cordialement,

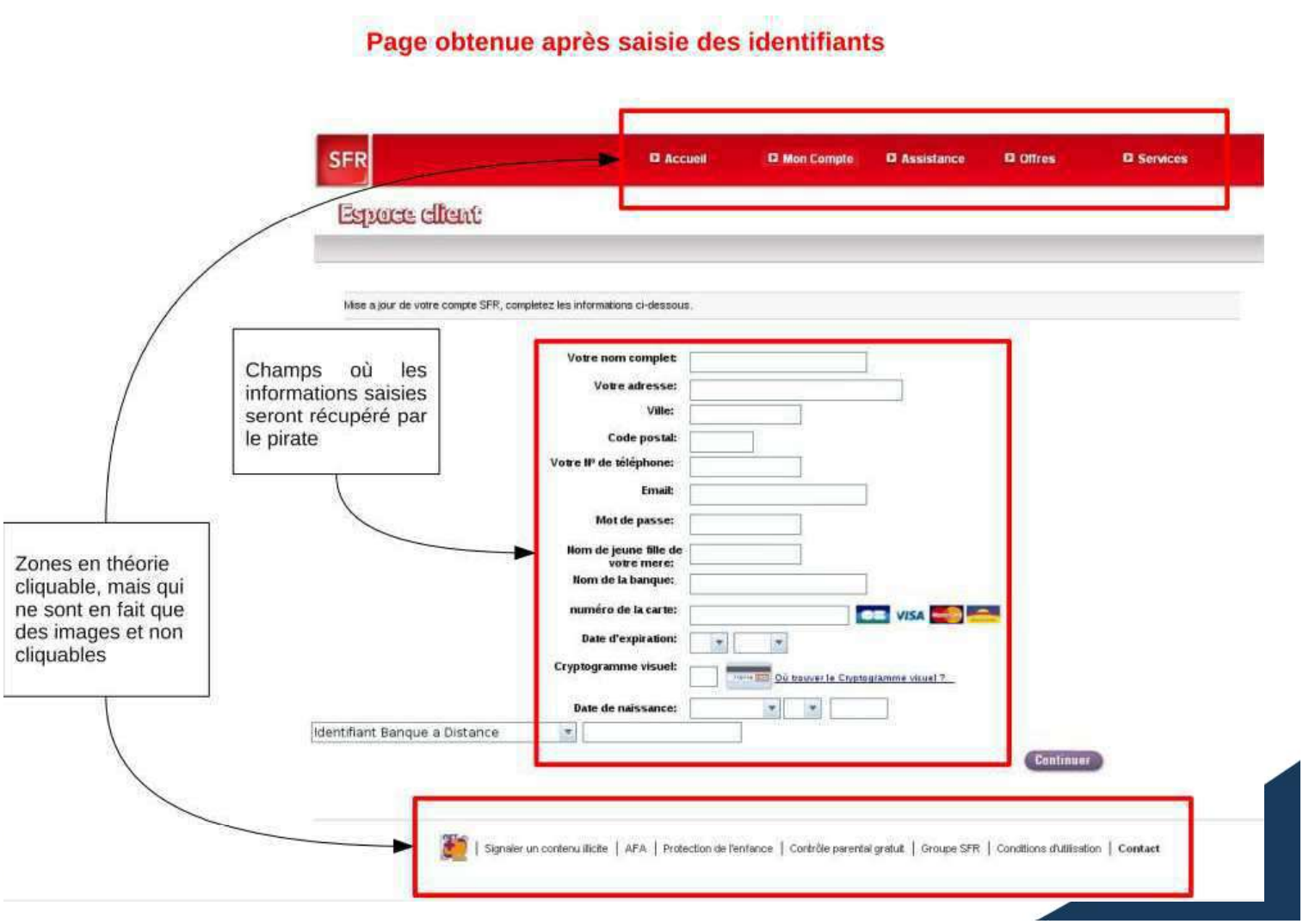
Dominique Remond,
Directeur Service Client

*En cas de non reponse a ce message, notre service decline toute responsabilite juridique au non réglement de votre impayée.

Université de Limoges



Université de Limoges



Courriel – Filoutage (3)

- Une banque ne va **jamais** vous envoyer un courriel pour vous dire de vous connecter à son site !
- Ne jamais se fier au visuel du site
- Si vous voulez aller sur le site de votre banque : utilisez l'adresse enregistrée dans vos favoris, ou tapez-la
- Observez bien l'URL (adresse web) : est-elle numérique ? Le nom est-il le bon ? Attention aux noms qui ressemblent, à rallonge
  - http://90.20.32.67/http/www.bnp.fr/
  - http://www.bnp.fr@www.sitecorrompu.com/
  - http://www.bnpfr.to/

Courriel – Filoutage (4)

- Mesures intégrées aux clients de messagerie : sous Thunderbird, menu `Outils` → `Options`, partie `Sécurité`, onglet « `Courrier frauduleux` », cocher « `Signaler si … susceptible d'être frauduleux` »
- Mesures intégrées aux navigateurs : vous avertissent si le site visité est répertorié comme frauduleux
  - sous Firefox : menu `Outils` → `Options`, partie `Sécurité`, cocher « `Bloquer les sites … d'attaque` » et « `Bloquer les sites … de contrefaçon` »
  - Existe aussi sous Chrome ou Internet Explorer 8
- A l'université : le contenu des mails est vérifié. Un lien www.banque.fr qui redirige vers un autre site sera noté :
  `Mailscanner soupçonne le lien suivant d'être une tentative de phishing`

Plan

Surfer sur le web

- Naviguer sur la toile (le *web*) peut présenter des risques
- On peut aller dans un endroit où des individus ou des organisations peuvent vous attaquer, vous tenter, vous arnaquer, etc.
- Comment se protéger ?

Surfer – Quelques protections

- Exercer son esprit critique (encore et toujours)
- Pré-requis : les « fondamentaux »
- Utiliser un navigateur alternatif, moins attaqué qu'Internet Explorer (40/50% des parts de marché) : Mozilla Firefox (20/30%), Safari (5/10%), Opera (2%), Google Chrome (15/25%)

Surfer – Le *phishing*

- Filoutage (*phishing*) : traité dans la partie « Courrier électronique »
- Attention, on peut se retrouver sur un site de phishing en suivant des liens sur le web, pas forcément en partant d'un courriel

Université de Limoges

Surfer – Les fenêtres surgissantes

- Les navigateurs peuvent bloquer les fenêtres publicitaires (*popup*)
- Ca ne protège pas forcément, mais c'est plus agréable ☺

Université de Limoges

Surfer – Mot de passe

- Les navigateurs peuvent se « souvenir » des mots de passe
- Ils sont enregistrés dans un « magasin »
- Conseil : ce magasin **doit** être chiffré avec un « super » mot de passe. Dans Firefox : menu `Outils` → `Options`, partie `Sécurité`, case `Utiliser un mot de passe principal`
- Certains sites enregistrent votre connexion, avec un *cookie* :
  - Pratique (pas besoin de se réauthentifier)
  - À utiliser avec précaution (surtout sur un PC public !)

Fondamentaux – Mot de passe

- De plus en plus de mots de passe à retenir
- Si on dérobe un mot de passe (avec un logiciel espion, parce qu'un site s'est fait volé ses données) : réduire le risque en utilisant des mots de passe différents
- Stratégie : utiliser le même mot de passe pour des niveaux de sécurité identique. Exemple : un pour les sites « bidons » ou pas important
- Construire un mot de passe : Tres-Fa-Ci-Le, Ce+diffisil, lavies1lofltr (**la** **vie** **est** **1** **lo**ng **fl**euve **tr**anquille)
- Vérifier sa complexité : https://www.microsoft.com/fr-fr/security/pc-security/password-checker.aspx
- Ne pas prendre un mot du dictionnaire
- A l'université : un seul compte pour tous les services numériques ⇒ **il est confidentiel**

Surfer – Bloquer les flash et les pubs

- Animations flash : partie d'un site web qui utilise *Flash Player*
- Des *modules* à ajouter pour Firefox ou Chrome, bloquent les flashs et les bannières publicitaires
- Exemples pour Firefox (`Outils` → `Modules complémentaires`) : *Flashblock* et *Adblock Plus*
- On peut en général cliquer pour déclencher la lecture du flash / de la pub si on veut
- Double avantage
  - « Allège » certains sites
  - Évite des attaques (sur les images, sur flash player)

Surfer – Utiliser « WOT » (Firefox et IE)

- WOT : WebOfTrust (réseau / web de confiance) http://www.mywot.com
- Composant à ajouter à Firefox, Chrome ou IE
- Gratuit
- Avertit quand on va sur un site « dangereux »
- Avertit quand un résultat d'un moteur de recherche est dangereux
- Basé sur des notes données par les internautes – manipulable ?
- Contrôle parental inclus

Surfer – Internet Explorer et les « ActiveX »

- Certains sites webs utilisent des « contrôles ActiveX »
- Exemple : antivirus en ligne
- Ne fonctionnent qu'avec Internet Explorer
- Composant logiciel envoyé par le site, qui s'exécute sur votre machine
- Potentiellement dangereux !
- IE (configuration par défaut) devrait demander l'autorisation, dans un bandeau jaune en haut de la page
- Ne l'accepter que si vous savez ce que vous faites

Surfer – Les traces

- Quand on navigue d'un site A à un site B en cliquant sur un lien, le site B reçoit l'information « vient du site A »
- Quand on va sur un site, celui-ci connaît votre adresse IP (et donc votre localisation géographique)
- Le navigateur transmet des informations : version de système d'exploitation, langue
- Le navigateur enregistre un historique des sites visités, des données rentrées dans les formulaires
- La navigateur stocke une copie des pages visitées (*cache*)
- Les *cookies* permettent à un site A de stocker des informations, sur votre PC : nom d'utilisateur, autorisations d'accès, nombre de connexions au site, etc.
  - Un site B ne peut pas accéder aux cookies de A
  - Sur un ordinateur public : effacer les cookies !

Surfer – Les traces (2)

- Les équipements du réseau (routeurs) sont des nœuds d'interconnexion du trafic : ils peuvent garder une trace des adresses IP, voir intercepter le contenu des échanges
- Les FAI ont l'obligation de garder pendant un an les traces des connexions Internet (décret 2006-358 du 24 mars 2006), pour les besoins de la justice
- Des solutions d'anonymisation (par exemple « Tor », proxy d'anonymisation) : présente ses propres dangers (un point de passage qui peut vous espionner !)

Surfer – Effacer ses traces locales

- Sous Firefox : menu `Outils` → `Supprimer l'historique récent`
- Pour effacer systématiquement : menu `Outils` → `Options`, partie `Vie privée`, choisir comme règle de conservation « `Utiliser les paramètres personnalisés pour l'historique` » et cocher « `Vider l'historique lors de la fermeture de Firefox` »

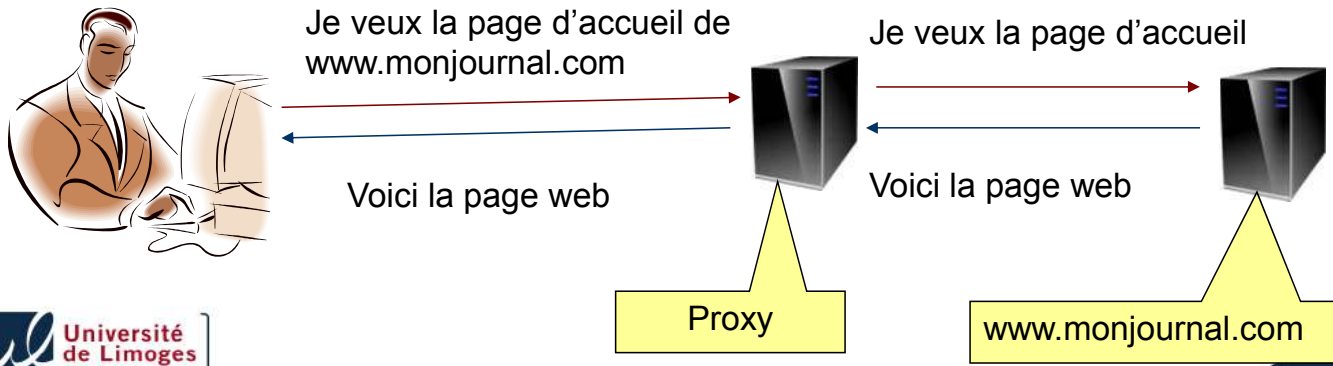
Surfer – Mode privé et traces locales

- Des navigateurs ont une fonction de navigation en mode « privé »
  - Pas d'historique de navigation
  - Pas d'historique des téléchargements
  - Pas de cookie enregistré
  - Pas d'historique des formulaires
- Plus de trace locale, mais vous laissez toujours une trace sur Internet
- Sous Firefox, menu `Outils` → `Commencer la navigation privée`

Université de Limoges

Surfer – Proxy d'anonymisation

- Un mandataire (*proxy*) agit à votre place
- Pour le web : il demande la page web à votre place, le site distant ne « voit » que le mandataire
- Il existe des proxy ouverts et gratuits/payants
- Pouvez-vous avoir confiance ?



Université de Limoges

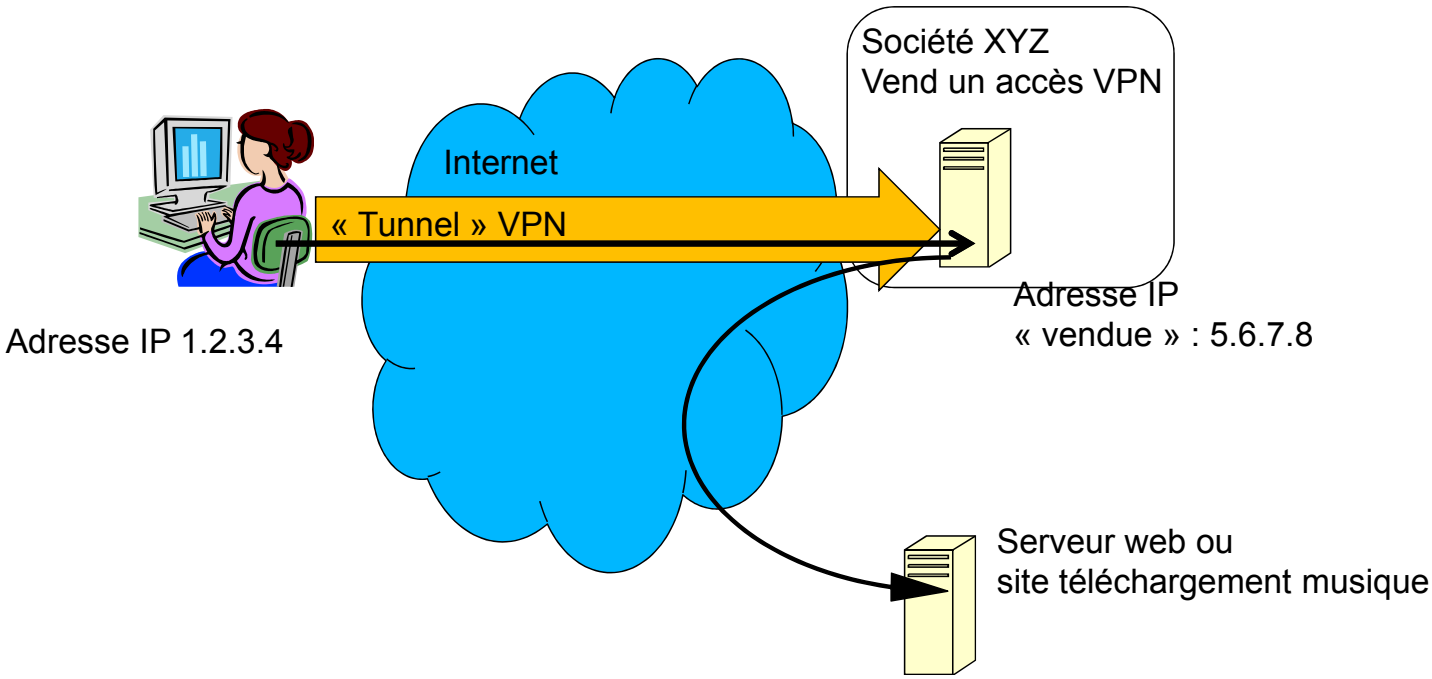
VPN Anonyme

- Un VPN (*Virtual Private Network*) établit un liaison (*tunnel*) entre votre PC et un autre réseau
- Le tunnel est peut-être chiffré (protection de la confidentialité)
- Vous obtenez une nouvelle adresse IP sur ce réseau
- Pour aller ensuite sur Internet, tout transite par le tunnel, et semble ensuite provenir de cette nouvelle adresse IP
- Des sociétés, localisées parfois dans des pays exotiques, vendent des accès VPN, utilisés pour se protéger des « gendarmes » d'Internet
- Comme si vous mettiez une lettre dans une lettre :
  - Vous voulez expédier une lettre
  - Vous la mettez dans une enveloppe avec l'adresse du destinataire final
  - Vous mettez la première enveloppe dans une deuxième, avec l'adresse d'un complice
  - Le complice ouvre la première enveloppe et re-expédie l'enveloppe interne

VPN anonyme (2)

- Vous êtes « caché » ; enfin, peut-être :
  - Quelles traces garde le complice ?
  - Est-ce qu'il ouvre l'enveloppe intérieure ?

VPN : schéma



La connexion vers le serveur sur Internet passe par le tunnel, et le serveur voit arriver l'adresse IP 5.6.7.8

Université de Limoges

Surfer – Protection des mineurs

- Principe technique : bloquer des sites, soit parce qu'ils sont connus pour leur contenu pornographique, haineux, etc. soit en fonction de mots clés
  - Liste blanche : on n'**autorise** que certains sites, tout le reste est **bloqué**
  - Liste noire : on **bloque** certains sites, tout le reste est **autorisé**
- Tous les FAI français fournissent un contrôle parental gratuit
- http://www.e-enfance.org/enfant-internet.php?page=3
- Autres logiciels :
  - K9 Gratuit http://www1.k9webprotection.com/
  - Payants : Optenet, Parental Filter 2, ...
- D'autres outils permettent de limiter l'accès à certaines heures, d'empêcher la transmission d'information personnelles …

Université de Limoges

Surfer – Protection des mineurs (2)

- Difficile de bloquer 100% des contenus
- Multiplicité des canaux : sites webs, P2P, messagerie instantanée, newsgroups
- L'éducation plus que l'interdiction ?
- https://www.internet-mineurs.gouv.fr/
- http://www.mineurs.fr
- http://www.commentcamarche.net/download/controle-parental-94

Surfer – Payer sur Internet

- Réputation du site visité, confiance : un élément important
- Complexité du droit international : en cas de litige, il sera beaucoup plus facile de faire intervenir la loi si l'entreprise est française
- HTTPS : nécessaire, avec ses limites
  - Basé sur des certificats
  - Vérifie l'identité du *site* ; mais on peut facilement créer un certificat, ou en acheter un (ne prouve pas l'honnêteté du site !)
  - Crée un canal « sécurisé » du poste au serveur (on ne peut pas écouter la conversation)
  - Ce n'est pas parce que la *connexion* est sécurisée qu'on ne risque rien. Le plus grand risque est de se sentir complètement en sécurité alors qu'on ne l'est pas

Surfer – Payer sur Internet (2)

- Payer avec une carte bleue temporaire et virtuelle :
  - Exemple : e-cartebleue de Visa (disponible à la Banque Populaire, Caisse d'épargne, …)
  - Problème si on a besoin de la même carte plusieurs fois ou physiquement (ex. à la SNCF, pour retirer le dossier)
  - Refusé par certains sites
- Payer avec une carte « pré-payée » d'un montant limité : NeoSurf (disponible chez les buralistes)
- Avec un porte-monnaie virtuel (MyNeoSurf) : peu de site les accepte en général
- Par virement bancaire : gratuit ou payant selon votre banque
- Remise contre-remboursement

Surfer – Payer sur Internet (3)

- Paiement par tiers de confiance : ne pas donner son numéro de CB au marchand
- Paypal (le plus connu, appartient à eBay), Paybox
  - Offre parfois une garantie en cas de non livraison du produit
  - Limite : pas « standard », mais fiable. Plutôt adapté pour des petits sites, pour faire des dons ?
- Internet+ :
  - Si votre FAI est compatible : Alice, Free, Orange, SFR
  - Si le site marchand l'accepte
  - Votre achat est débité sur votre facture Internet
- Buyster par Orange, Bouygues, SFR :
  - Si le site marchand l'accepte
  - Associe votre CB a votre téléphone portable

Surfer – Payer sur Internet (4)

- Que dit le droit ?
  - 2 clics : un pour la commande, un pour confirmer
  - Le site doit accuser réception de la commande
  - Délai de rétractation : 7 jours francs
  - Obligation de résultat, et commande exécutée sous 30 jours
- En cas de litige :
  - Mieux vaut que le site marchand soit en France
  - Faire valoir ses droits rapidement, par lettre recommandée
- http://www.payerenligne.com

Plan

- Avant-propos
- Qu'est-ce que « Internet » ?
- Internet et droit
- Les logiciels malveillants
- Le courrier électronique
- Le web
- Autres usages (P2P, jeux, réseaux sociaux, …)

Les réseaux sociaux

- Les sites de « réseaux sociaux » (Facebook : 500 millions de compte revendiqués) permettent de communiquer, de créer des liens
- Qui est en face ? Quelles informations réelles donner ?
- Comment avoir confiance dans la **sûreté** du site : est-ce qu'il peut se faire voler vos données privées ?
- Comment avoir confiance dans **les pratiques du site** : vend-il des informations sur vous ? Avez-vous lu les conditions d'utilisation ? Comment peut-on supprimer les données personnelles récoltées ?

Messagerie instantanée

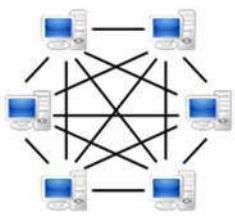
- MSN / Windows Live Messenger, Google talk, AIM, ICQ, Yahoo! Messenger
- A la base : communication sous forme textuelle, **instantanée** (*chat*)
- Maintenant : avec webcam, échange de fichiers
- Utilisé pour des attaques de phishing, des vols d'identifiant, créer des rencontres, ou par des virus dédiés
- Des outils spéciaux pour effacer ces virus
  - Exemple : http://www.viruskeeper.com/fr/clean_virus_msn.htm
- Outils de vérification MSN : MSN Checker Sniffer (moyen)

Les mondes virtuels

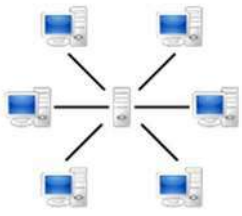
- Archétypes : Second Life, WoW
- De l'argent virtuel, des possessions (objets, territoires) virtuelles
- Mais qui se convertissent en argent réel
- Des virus / logiciels, ou des « armées » de jeunes recrutés pour « écumer » ces territoires ...

Surfer – Le pair-à-pair

- *Peer-to-peer*, P2P
- Principe : communication directe d'internaute à internaute, sans passer par un « serveur »
- Inventé pour échanger, partager des fichiers
- Exemples : Kazaa, emule, edonkey



Système P2P sans serveur central



Système avec serveur central

Surfer – Le pair-à-pair (2)

- Les échanges de fichiers sont soumis à la législation
- Le contenu n'est jamais garanti : un logiciel piraté proposé au téléchargement peut cacher un Troyen !
- A l'université : la charte d'usage des réseaux réserve en priorité l'usage à l'éducation et à la recherche

Sites utiles

- Droit et Internet :
  - http://www.alain-bensoussan.com/
  - http://www.legalis.net/
  - http://www.cnil.fr/
  - http://www.irccyn.ec-nantes.fr/~magnin/publications/sreti/SRETI_Droit.pdf
  - http://www.droitsurinternet.ca/ (Québecois)
- http://support.microsoft.com/gp/lifecycle : Politique de Support Microsoft
- http://www.microsoft.com/security ou http://www.microsoft.com/france/securite/ : le portail de la sécurité chez Microsoft
- http://www.foruminternet.org/ : des conseils et du droit
- http://www.protegetonordi.com : pour les enfants, par les pouvoirs publics et Microsoft
- http://www.securite-informatique.gouv.fr/ : portail de la sécurité informatique du gouvernement

Quelques références

- Rue89, «Ces rumeurs islamophobes grossières qui polluent le Net » http://www.rue89.com/le-demonte-rumeur/2010/03/05/ces-rumeurs-islamophobes-grossieres-qui-polluent-le-net-141472
- Statistiques d'usage des navigateurs : http://gs.statcounter.com/