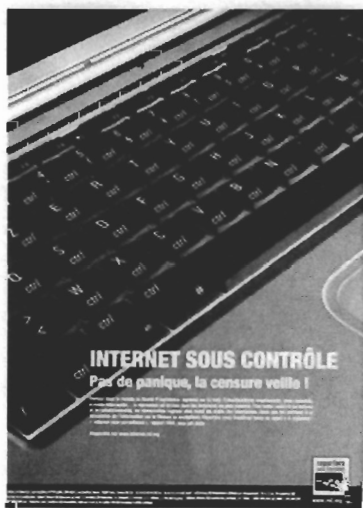


SURFEZ SANS VOUS MOUILLER

Chaque utilisateur d'Internet en général – le journaliste en particulier – doit pouvoir protéger sa vie privée et assurer la confidentialité de ses communications. Quels sont les dangers de l'utilisation d'Internet et comment mieux se protéger?



Poster de Reporters sans Frontières

«N'écrivez pas sur Internet ce que vous n'écririez pas sur le dos d'une carte postale»

Gérard Demaretz
Cyber-espionnage

«Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety.»

Benjamin Franklin, 1755

TABLE DES MATIERES :

INTRODUCTION :	4
IERE PARTIE: ANALYSE	5
Des origines d'Internet à la naissance du World Wide Web	5
L'évolution d'Internet: le Web 2.0	6
Les problèmes de sécurité d'Internet	7
Conflits dans le cyberspace – les principaux acteurs	8
Les dangers (menaces et attaques)	9
<i>Non-techniques – indépendants du degré de sécurité informatique</i>	9
<i>Techniques - dépendants du degré de sécurité informatique</i>	10
<i>Nomenclature officielle des cyberattaques</i>	11
Les sacro-saintes règles de sécurité	12
<i>L'ordinateur</i>	12
<i>Les accès</i>	12
<i>Les transmissions</i>	12
Où stocker ses données: local ou serveur?	13
La confidentialité des données enregistrées: chiffrage et effacement	13
Quelques configurations possibles avec leurs niveaux de sécurités minimums	14
<i>Pour un usage quotidien</i>	14
<i>Pour un usage journalistique sensible (exemple : enquête sur un réseau terroriste ou sur la fabrication de « pipe bombs »)</i>	14
<i>Si vous êtes le nouveau «James Bond»</i>	15
BIBLIOGRAPHIE	17
CONTROLE D'EDITION	17
LICENCE CREATIVE COMMONS	17

A V E R T I S S E M E N T :

L'auteur de ce document nomme des entreprises (éditeurs de logiciels, propriétaires de sites Web, fournisseur d'accès Internet, sociétés d'hébergement), des services de renseignements et de répression du crime organisé, des organisations cybercriminelles et de réseaux terroristes dans un but purement informatif et éducatif.

Ce document ne formule aucun jugement ni d'ordre commercial ni d'ordre politique.

De par le caractère dynamique d'Internet, certains liens proposés en notes de bas de pages peuvent être indisponibles au moment de la lecture de ce document.

L'auteur n'assume aucune responsabilité quant aux conséquences possibles de l'utilisation de services Web et de logiciels abordés dans ce document.

INTRODUCTION :

Chère lectrice, cher lecteur,

Sommes-nous conscients des dangers que nous courrons en utilisant Internet et savons-nous nous protéger?

Vous n'êtes ni technicien, ni informaticien mais vous surfez sur Internet en tapant sur un clavier d'ordinateur et en cliquant avec une souris? **Ce document est écrit pour vous!**

Au 21^{ème} siècle, la question de la vie privée¹ et de son respect repose sur un vrai paradoxe.

D'une manière générale, nous souhaitons faire respecter une part d'ombre sur nos habitudes, nos fréquentations, nos origines, notre cercle familial, notre religion, notre orientation sexuelle, notre situation financière, notre santé, etc. La notion de protection des données personnelles est une résultante du besoin d'intimité de l'être humain dans notre société.

Paradoxalement, nous faisons preuve d'une attitude insouciance lorsque nous utilisons les nouvelles technologies. Nous avons des conversations intimes avec nos téléphones portables. Nous choisissons des mots de passe simplistes que nous notons sur le coin de notre écran. Nous n'hésitons pas à transmettre des informations commerciales confidentielles dans des courriels (messages électroniques – e-mails).

Certains d'entre-nous ont des attitudes carrément exhibitionnistes dans leurs blogs sur des réseaux de socialisation (Facebook, etc.). Ils y dévoilent nom et prénom, date et lieu de naissance, scolarité, photographies ou vidéos, même parfois le cercle de leurs amis et connaissances, leurs intérêts, leur profession, etc.

Après recherches et recoupements, il est facile de construire le profil complet d'un internaute comprenant adresse, numéros de cartes bancaires, etc.

Certaines personnes ou organisations n'hésitent pas à se servir d'Internet pour tirer parti, légalement ou illégalement, de ces informations.

Ce document est divisé en deux volets:

- une **partie analytique** informe le lecteur de la nature d'Internet, de son fonctionnement, des conflits dans le cyberspace, des principaux acteurs et des menaces et dangers encourus
- une **partie pratique** présente des possibilités et des outils disponibles pour mieux se protéger.

Je vous remercie d'ores et déjà de vos commentaires et vous souhaite bonne lecture.

Christian Brülhart

UniNE – FLSH (Journalisme et histoire)

(christian.brulhart@unine.ch ou christian.brulhart@gmail.com)

¹ La 30ème conférence mondiale de protection des données et de la vie privée se tiendra à Strasbourg, lieu hautement symbolique de l'histoire du 20ème siècle, dans l'hémicycle du Conseil de l'Europe, du 15 au 17 octobre prochain. Elle portera sur le thème «Protéger la vie privée dans un monde sans frontières». Cette conférence est organisée, pour la première fois, conjointement par les Commissions française et allemande qui fêtent, ensemble, leur 30ème anniversaire en 2008.

IERE PARTIE: ANALYSE

Des origines d'Internet à la naissance du World Wide Web²

Internet (**Inter-networking**) est une invention de la guerre froide des années 1960. Dans un contexte général tendu de confrontation des deux blocs marxiste et capitaliste, cette réalisation serait une réaction militaire américaine à une nouvelle menace soviétique sur les Etats-Unis suite à l'envoi du satellite Spoutnik en orbite.

En effet, l'armée américaine, craignant de voir son espace territorial directement menacé par le survol de satellites ennemis lançant des attaques surprises à l'arme atomique, voulait assurer ses transmissions informatiques entre les divers centres de commandements stratégiques et les sites de tir de missiles nucléaires.

Le réseau Milnet (**Military Network**) et ARPANET (**Advanced Research Project Agency Net**) reliait plusieurs ordinateurs délocalisés. Grâce à un langage développé par le Pentagone, ceux-ci resteraient connectés, par un réseau de câbles, même lorsque certaines lignes de transmission seraient détruites.

Cette méthode de transmission évolua et donna naissance, après plusieurs mutations, au langage TCP/IP (**T**ransfer **C**ontrol **P**rotocol / **I**nternet **P**rotocol). Contrairement au téléphone, qui nécessite la connexion physique de circuits pour transmettre la voix (circuit switched networking), l'information transmise par Internet est partagée en plusieurs morceaux et est envoyée sous forme de paquets (packet switched networking). Ceux-ci «voyagent» vers le destinataire par divers chemins régulés par des sortes de policiers de la circulation : les routeurs (routers). A l'arrivée dans l'ordinateur destinataire, les divers morceaux sont «recollés» et l'information est ainsi reconstituée.

Le langage TCP/IP possède aussi une caractéristique qui assurera son succès planétaire: il permet à des machines totalement différentes de communiquer. C'est en quelque sorte un «esperanto» électronique, langage que tous les ordinateurs du monde parlent et comprennent.

Le World Wide Web (www ou Web), un composant d'Internet, est inventé en 1989 au CERN par Tim Bernes-Lee. Ce chercheur développe le langage hypertexte (**H**ypertext **T**ransfer **P**rotocol – http) qui permet de relier plusieurs documents au moyens de liens électroniques (links).

Le phénomène du Web explose lorsque le président Bill Clinton décrète l'ouverture d'Internet aux organismes commerciaux en 1994.

Plusieurs services sont disponibles sur Internet, comme diverses catégories de véhicules peuvent circuler sur une route. Les plus connus, le Web mis à part, sont la messagerie électronique (e-mail), le clavardage (chat), la téléphonie et la visioconférence.

² Internet Society, Histories of the Internet : <http://www.isoc.org/internet/history/>

L'évolution d'Internet: le Web 2.0³

A l'origine, le webmestre (webmaster), était la personne qui s'occupait de la publication d'informations sur le Web. Elle devait acquérir des compétences techniques et connaître l'utilisation d'outils informatiques particuliers.

A part quelques exceptions comme les services de courriel en ligne (Gmail, Hotmail ou YahooMail), les services de ventes aux enchères (eBay) ou les plateformes d'échange d'opinions (Bulletin Board Systems), le flux d'informations publiées était certes important mais allait dans un seul sens: de l'éditeur (rôle actif) au lecteur (rôle passif).

Grâce à l'évolution foudroyante des technologies de l'information, le Web participatif est né. Avec de nouveaux outils (Wiki), qui ont remplacé les anciens systèmes de gestion de contenu (Content Management Systems), pratiquement n'importe quel lecteur d'un site Web peut publier sa contribution, si l'accès lui est donné.

Voici un exemple de l'évolution : Web 1.0 : la *homepage* est une sorte de présentation personnelle statique (un CV en ligne) → Web 1.5 : le *weblog* ou *blog* est un journal intime en ligne → Web 2.0 : *myspace* ou *facebook* devient un réseau social

Cette évolution permet un double flux, ajoutant au rôle passif du lecteur celui actif du contributeur, de l'éditeur. Ce changement, multiplié par le phénomène du « crowdsourcing », a généré une explosion d'informations publiées sur la toile.

Voici quelques exemples de nouveaux services basés sur le système collaboratif (la liste n'est pas exhaustive):

- *Wikipédia*: Encyclopédie où les articles sont rédigés par des internautes
- *Facebook*: Réseau social qui relie amis, collègues de travail et connaissances
- *Flickr* : Service de mise en ligne de photographie
- *YouTube*: Site permettant d'envoyer et de partager des vidéos
- *AgoraVox*: Agence de presse sur Internet où le citoyen joue le rôle de reporter/journaliste
- *LinkedIn*: Site de réseautage professionnel

³ Web 2.0 : mythe et réalité <http://xmlfr.org/actualites/decid/051201-0001>

W3Québec, Qu'est-ce que le web 2.0 ? : <http://w3qc.org/presentations/20060130/>

Web 2.0 : la révolution par les usages http://www.journaldunet.com/solutions/0601/060105_tribune-sqli-web-20.shtml

What Is Web 2.0 <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html>

Getting Started with Web 2.0 <http://mediatedcultures.net/ksudigg/?p=103>

Les problèmes de sécurité d'Internet⁴

Mise-à-part l'utilisation de la technologie par l'homme qui peut, comme tout autre outil, être utilisé à dessein criminel, pourquoi Internet souffre-t-il de problèmes de sécurité récurrents?

Une partie de la réponse se trouve dans l'origine et la nature d'Internet. Avant d'évoluer en réseau des réseaux, cette infrastructure a tout d'abord été pensée pour une utilisation exclusivement militaire, c'est-à-dire dans un environnement clos. Les machines connectées ont été prévues pour communiquer sur une base de confiance (trusted connection) puisqu'elles étaient utilisées par du personnel de l'armée américaine dans l'exercice de sa mission.

Internet n'est pas une infrastructure compacte. Bien au contraire, il est construit au moyen d'un assemblage de composants hétéroclites, où chacun a une fonction bien particulière. Transmission de signaux par câbles ou ondes, paquets d'informations en code binaires, passerelles (gateways), routeurs (routers), serveurs de noms de domaines (DNS), serveurs de messagerie, serveurs web, serveurs FTP, autant de composants présentent autant de possibilités d'accès illégaux. Plus une maison présente d'ouvertures, plus les possibilités d'infractions sont nombreuses. Logique non ?

A cela s'ajoute un phénomène de diversification des types d'ordinateurs connectés. Jusque dans les années 90, la plupart des systèmes, appelés ordinateurs personnels (Personal Computers - PC), avaient été construits dans l'idée de produire une machine à traitement de texte (éventuellement un tableur), donc pour ne satisfaire les besoins que d'un seul usager. Il n'y avait pas de possibilité de créer des profils d'utilisateurs différents, comme administrateur ou visiteur sur le même système. Ces machines se trouvaient «seules sur une île», sans possibilité de communiquer entre elles. Elles devaient être modifiées pour pouvoir se connecter. Par exemple, les PC avec Windows 3.1 (1994) devaient recevoir une carte de réseau et un ajout de programmes (winsock) pour être capables de comprendre le langage d'Internet (protocole TCP/IP).

Comme évoqué plus haut, l'ouverture graduelle d'Internet aux organisations académiques, puis aux entreprises commerciales et finalement aux individus a changé la donne. La diversification des utilisateurs a forcément entraîné des dérives. Partie d'entre eux sont des gens mal intentionnés.

Dans le monde virtuel, comme dans le monde réel, il existe des voleurs, des terroristes, des pédophiles, etc.

⁴ Liste des sujets de sécurité informatique sur un site d'information : <http://www.spyworld-actu.com/spip.php?rubrique4>

Les géants de l'Internet mondial corrigent une grave faille de sécurité : <http://www.lesechos.fr/info/comm/300279144.htm?xtor=RSS-2004>

Conflits dans le cyberspace – les principaux acteurs

L'utilisateur commun d'Internet n'a absolument aucune idée de la vie «underground» de la toile.

Les menaces criminelles sur la vie privée ou sur le patrimoine d'une personne, qui jadis étaient limitées géographiquement et temporellement, se sont étendues au monde entier et sont présentes 24 heures sur 24, 7 jours sur 7, 365 jours par an.

Facteur encore plus inquiétant, certains gouvernements commencent à peine à avouer leur impuissance à assurer la protection de leurs infrastructures⁵ (cyberattaque), celles des entreprises «à risque» (cyberintelligence économique) et celle de leurs citoyens⁶ (cybercrime). En conséquences, certaines entreprises ou organisations non-gouvernementales se sont spécialisées dans ces activités⁷.

Les outils de protection des personnes, tels que le cadre légal, les organismes de surveillance, de protection et de défense sont complètement dépassés faute de prise de conscience des politiques et dirigeants. Nos gouvernements ont encore grand peine à assurer un financement qui permette d'adapter nos infrastructures et nos services étatiques pour lutter efficacement contre les menaces liées à l'existence d'Internet.

Du côté des «gentils» se trouvent certains organismes comme la National Security Agency⁸ (NSA) ou European Enforcement Police⁹ (EnfoPol) qui sont chargés de la surveillance et de la répression de la cybercriminalité et du cyber terrorisme. Ils sont également chargés de lutter contre une guerre électronique (cyberwar) qui peut être lancée par un Etat contre certains autres¹⁰. Les Etats-Unis sont en train de mettre sur pied un nouveau projet, dirigé par le DARPA, destiné à entrevoir Internet comme un «réel» théâtre d'opération militaire¹¹.

Une multitude d'agences de renseignement, souvent cachées dans des organigrammes d'administrations sous des noms peu évocateurs ou des entreprises financées par des fonds étatiques non-budgétés, se chargent de la surveillance des communications mondiales.

La plus impressionnante est probablement la célèbre NSA basée à Fort Meade, dans l'Etat du Maryland. Grâce à son réseau *Echelon*¹² de satellites espions et stations terrestres d'écoute, cette

⁵ France : Le Sénat met en garde contre la vulnérabilité des systèmes d'information de l'État <http://www.spyworld-actu.com/spip.php?article8218> Rapport de Cyberdéfense du Sénat FR : <http://www.senat.fr/rap/r07-449/r07-4491.pdf> Cyber-défense : la France accuse "un réel retard" : <http://www.spyworld-actu.com/spip.php?article8229> CERTA : Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques : <http://www.certa.ssi.gouv.fr/>

⁶ Royaume-Uni : Internet Security: <http://www.publications.parliament.uk/pa/ld200708/ldselect/ldsctech/131/131.pdf>
Commentaire: <http://www.lightbluetouchpaper.org/2008/07/08/personal-internet-security-follow-up-report/>
Papier de la BBC: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk_politics/7495118.stm

⁷ Centre de sécurité informatique: <http://www.secuser.com/>
The Shadowserver Foundation: <http://www.shadowserver.org/wiki/>

⁸ National Security Administration (USA) : <http://www.nsa.gov/about/index.cfm> et son réseau d'écoute "Echelon" <http://www.fas.org/irp/program/process/echelon.htm>

⁹ EnfoPol: Toute l'activité d'EnfoPol sur ZDNet.fr: <http://www.zdnet.fr/tag/enfopol/>

¹⁰ Cyberdéfense : un nouvel enjeu de sécurité nationale <http://www.spyworld-actu.com/spip.php?article8232> et le rapport du Sénat français : <http://www.senat.fr/rap/r07-449/r07-4491.pdf>

¹¹ Etats-Unis – The National Strategy to Secure Cyberspace: <http://www.whitehouse.gov/pcipb/>

Nouveau projet du DARPA: <http://infowars.net/articles/may2008/060508DARPA.htm>

et RFC du projet: <https://www.fbo.gov/utills/view?id=c330660f00c9820d05c9f4c5>

¹² Réseau *Echelon*: <http://reseau.echelon.free.fr/reseau.echelon/>

organisation pratique une veille à l'échelle planétaire sur toutes les communications (lignes téléphoniques, GSM, satellite, Internet).

Concrètement, il suffit qu'un mot particulier (tag), introduit dans une banque de données de mots clés, soit écrit ou prononcé puis transmis électroniquement d'un point A à un point B dans le monde, que le système d'écoute *Echelon* le repère et que les puissants ordinateurs de la NSA l'analyse. Cet échantillon est alors comparé à des milliards d'autres. Le processus, répété un nombre incalculable de fois, génère des profils qui sont ensuite soumis à une analyse humaine.

Du côté des «méchants», la situation n'est pas moins inquiétante. Les pirates informatiques (hackers), qui au départ opéraient individuellement et qui étaient parfois plus motivés par un esprit de défi que de lucre, se sont professionnalisés et fédérés¹³. Certains ont été «récupérés» par le crime organisé ou par des réseaux terroristes, d'autres ont été engagés par des agences de renseignements et le reste se sont recyclés comme consultant de sécurité informatique.

Les dangers (menaces et attaques)¹⁴

Seuls les dangers concernant les usagers (individus) sont abordés ci-après.

Non-techniques – indépendants du degré de sécurité informatique

- Le *scam* est une fraude¹⁵. Elle se présente généralement sous la forme d'un courriel qui propose de percevoir de l'argent pour le compte d'une tierce personne. En contrepartie, une commission substantielle est promise. Le résultat est généralement le détournement de l'argent qui était présent sur le compte car les criminels ont eu connaissance des coordonnées bancaires complètes.
- Le *phishing* (anglais) ou *hameçonnage* (français) est le vol des coordonnées de connexion à des services (financiers) en ligne. Par l'intermédiaire d'un message électronique qui prétexte généralement un contrôle, le destinataire est prié de se rendre sur le site de l'entreprise (par exemple une banque) en cliquant sur un lien. Il s'agit en fait d'un site factice reprenant la mise en page d'origine. L'utilisateur complète les champs « utilisateur » et « mot-de-passe ». Lorsqu'il confirme son choix, les informations sont alors envoyées aux pirates. Ceux-ci n'ont plus qu'à s'introduire sur votre compte et le vider.
- Le *vol de carte de crédit* se produit généralement en utilisant un formulaire de paiement non-sécurisé lors d'achats en ligne. Les informations sensibles d'une carte bancaire de débit ou de crédit sont transmises, sans être chiffrées, et sont interceptées par des pirates. Ceux-ci s'en servent pour des achats et des retraits d'argent.
- Le *vol d'identité*¹⁶ est généralement le résultat de l'agrégation de données personnelles ouvertement publiées sur Internet. Puisées de diverses sources, elles permettent de

La Suisse se fait doubler par Echelon: <http://www.transfert.net/a2668>

¹³ Russian Business Network : http://en.wikipedia.org/wiki/Russian_Business_Network

¹⁴ Portail de sécurité informatique : http://fr.wikipedia.org/wiki/Portail:S%C3%A9curit%C3%A9_informatique

¹⁵ Plus d'information sur http://fr.wikipedia.org/wiki/Fraude_4-1-9. Pour une liste exhaustive des scams :

<http://www.scam.com/> (en anglais).

¹⁶ Vol d'identité (ID Theft): <http://www.idtheftcenter.org/>

fabriquer le profil complet d'une personne, ses habitudes de consommation y compris. Le but premier est généralement financier: demande de prêts, commande de cartes de crédit, etc. Néanmoins certaines entreprises achètent des adresses de consommateurs qui présentent un profil particulier (sexe, âge, formation, revenu, profession, etc.).

- Le *viol de la sphère privée*¹⁷ est un vol d'informations intimes. Celles-ci peuvent être publiées sur Internet ou privées, en lisant le courrier électronique par exemple. Ceci dans un but de chantage, de propagation de rumeurs ou d'organisation de vraies campagnes de dénigrement qui nuisent à la réputation de la personne. Exemple: vous travaillez dans une banque, vous êtes en compétition pour un poste à responsabilité et votre employeur découvre que vous avez des dettes de jeu...

Les réseaux sociaux¹⁸ et professionnels, où des personnes donnent une quantité d'informations personnelles (dates de naissance, hobbies, amis et famille, lieux de vacances) et professionnelles (formations, employeurs, fonctions, collègues) sont de vraies mines d'or pour les pirates. Ces remarques s'appliquent également aux entreprises¹⁹. Les réseaux sociaux deviennent une source importante de menaces pour la vie privée des internautes mais aussi pour des gouvernements²⁰.

Techniques - dépendants du degré de sécurité informatique

- Les *virus* sont des programmes informatiques introduits clandestinement dans un ordinateur dans le but de nuire l'utilisateur de l'ordinateur et d'en infecter d'autres. Ils peuvent être trouvés et détruits en utilisant un programme anti-virus.
- Les *malwares* définissent une catégorie générale de programmes informatiques malveillants, nuisibles à l'utilisateur dans un sens général. Les virus et les spywares font partie des malwares.
- Les *spywares* sont des programmes informatiques espions destinés à assurer l'accès d'un ordinateur à une personne non autorisée et/ou de collecter certaines informations contenues par un ordinateur (no. de comptes bancaires) ou introduites par l'utilisateur (mots-de-passe).
- Le *spam* ou *pourriel* est un message électronique contenant de la publicité non sollicitée. Envoyés par millions, ils surchargent les serveurs de messagerie et remplissent inutilement les boîtes de courriel.
- La *prise de contrôle* de votre ordinateur. Grâce à l'installation d'un *malware*, des pirates informatiques prennent le contrôle de votre ordinateur. Il peut y avoir plusieurs raisons.

¹⁷ Protection de la vie privée :

France : <http://www.cnil.fr/index.php?id=2433> (cf. note sous introduction)

Bon site général (en anglais): <http://www.privacylives.com/>

Exemple de cabinet spécialisé dans la réputation numérique : <http://www.web-reputation.com/>

¹⁸ Facebook : quand les applications tierces détournent vos données personnelles:

<http://www.zdnet.fr/actualites/internet/0,39020774,39382029,00.htm>

¹⁹ La gestion des données privées des salariés à revoir dans une majorité d'entreprises:

<http://www.zdnet.fr/actualites/informatique/0,39040745,39382101,00.htm>

²⁰ Europe : ENISA Position Paper No.1 Security Issues and Recommendations for Online Social Networks:

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

Suisse: Réseautage social sur Internet. Prudence et discrétion sont de mise :

<http://www.edoeb.admin.ch/dokumentation/00445/00471/01195/01198/index.html?lang=fr>

France: Les réseaux sociaux menacent-ils la sécurité nationale? <http://www.spyworld-actu.com/spip.php?article7780>

Soit les pirates (hackers) prennent en otage votre ordinateur et vous proposent de le «réparer» contre paiement, c'est-à-dire l'achat d'un programme informatique effaçant le *malware*. Soit les pirates ont d'autres ambitions en font un *zombie*. Ils vont relier votre machine à des centaines d'autres ordinateurs (botnets²¹) et vont l'utiliser à votre insu pour des opérations illégales d'envergure internationale (envois de spam, cyberattaques, etc.).

Nomenclature officielle des cyberattaques

Pour les services de lutte contre la cyberdélinquance et la cybercriminalité, les attaques sont classées en 6 catégories (privées et commerciales confondues)²²:

1. Le vol d'information pour usage personnel, la revente ou contre l'entreprise
2. L'atteinte à la vie privée (avec contrainte possible)
3. La fraude, le chantage et diverses escroqueries possibles
4. Le sabotage par destruction de données et de matériel
5. Prolifération de rumeurs déstabilisatrices
6. Modification de pages d'un site pour porter atteinte à la crédibilité de l'entreprise

²¹ Onze botnets contrôlent ... : <http://www.pcinpact.com/actu/news/42984-botnets-zombies-rsa-Srizbi-Bobax.htm>

²² Page 174, Desmaretz Gérard, Cyber-espionnage : ou comment tout le monde épie tout le monde!, Paris : Chiron, 2007, 252 pages

2^{EME} PARTIE : LES SOLUTIONS PRATIQUES

Les sacro-saintes règles de sécurité

Tous le monde le dit et le répète : suivez les règles de sécurité²³ et rien (ou presque rien) ne se passera. Chaque expert définit ses règles, des plus strictes au plus légères. Un point est cependant reconnu, *degré de sécurité* est généralement inversement proportionnel à *aisance de travail*.

En très résumé et simplifié, il faut assurer trois domaines principaux :

L'ordinateur

- (!) Ne **jamais** se connecter et **travailler** quotidiennement **comme administrateur** (ou profil équivalent)! N'utiliser ce profil, avec mot-de-passe d'ouverture de session, que pour des mises-à-jour, des modifications réseaux (Wi-Fi, ADSL), des ajouts de matériels et pour l'installation de programmes de confiance destinés à être utilisés par tous les utilisateurs partageant le même ordinateur. Si un pirate ou virus s'introduit dans l'ordinateur pendant une session ouverte avec le profil d'administrateur, il aura directement accès à tous les fichiers sensibles de la machine.
- Effectuer une **mise-à-jour** régulière (quotidienne) du système d'exploitation et du programme **anti-virus**.

Les accès

Un mot de passe facile à deviner équivaut à fermer la porte de son appartement à clef et de **laisser la clef sur la serrure**. Un mot de passe difficile à deviner n'est pas forcément difficile à mémoriser. Je vous recommande d'essayer la méthode «Diceware»²⁴ qui est extrêmement fiable.

Les transmissions

- Le réseau Wi-Fi: Si utilisé, il faut prendre le temps de le **chiffrer** et d'y mettre un mot-de-passe solide, quitte à le partager avec les autres utilisateurs du réseau. La responsabilité du propriétaire du réseau est engagée par la nature des informations qui y transitent (téléchargement pirate de musique, photographies pédophiles).
- Le pare-feu: Il faut l'activer sur le router/modem ADSL si possible. Il protégera ainsi tout le réseau local. Si cette option n'existe pas, le pare-feu de chaque ordinateur connecté doit être activé.

²³ Suisse - Protection de son ordinateur par le Préposé fédéral à la protection des données:

<http://www.edoeb.admin.ch/themen/00794/00928/00930/00949/index.html?lang=fr>

Les 10 commandements de la sécurité sur l'internet: http://www.securite-informatique.gouv.fr/gp_rubrique34.html

Sécurité: 60 erreurs à ne pas commettre : <http://www.journaldunet.com/solutions/securite/dossier/07/0910-60-erreurs-securite/1.shtml>

Les 12 conseils de l'EFF pour protéger votre vie privée: http://www.bugbrother.com/eff/eff_privacy_top_12.html

²⁴ Méthode « Diceware » pour créer des mots de passe:

(français) http://web.archive.org/web/20041012030451/www.gjldp.org/CHARENTAISES/article.php3?id_article=4

(anglais) <http://world.std.com/~reinhold/diceware.html>

- Le serveur proxy: Sans utilisation d'un proxy, il est impossible de rester discret. Tous les sites visités par l'utilisateur peuvent être répertoriés en déterminant le numéro IP, identifiant unique de chaque ordinateur connecté à Internet (permet la localisation donc l'identification²⁵).

Afin de minimiser les risques de pénétration du réseau local et des ordinateurs qui y sont reliés, il est conseillé de déconnecter physiquement le boîtier ADSL, par exemple pendant la nuit ou lors des absences. Le meilleur pirate ou la NSA ne pourra absolument rien faire (à part vous rendre une petite visite...).

Où stocker ses données: local ou serveur?

Cette question n'a pas de réponse définitive car chaque solution présente ses avantages et ses inconvénients. Ceci reviendrait à se poser la question quelle est la meilleure solution pour financer son logement: locataire ou propriétaire?

	Solution : «Local»	Solution : «Serveur»
Avantages:	Données disponibles sur l'ordinateur exclusivement	Données disponibles en mode «nomade»
Inconvénients:	Danger de perte de données en cas de problème d'ordinateur (disque dur ou virus). Données indisponibles en mode «nomade»	Données indisponibles en cas de panne de réseau et risque de perte de confidentialité

La confidentialité des données enregistrées: chiffrement et effacement

Dans le cas où les données stockées sur des médias (disque dur de l'ordinateur, espace de stockage en ligne ou clé USB) devaient être protégées, il est conseillé d'utiliser des programmes de cryptage de données²⁶. En cas d'utilisation d'un portable contenant des données sensibles (liste de contacts, documents, reportages, etc.), il est conseillé de créer une partition de «données», espace sur lequel toutes les informations enregistrées seront chiffrées.

Les données enregistrées sur un disque dur et effacées sont toujours disponibles, même en cas de reformatage du média. Un fichier placé dans la poubelle puis effacé de la poubelle reste stocké sur le disque. Seule la référence du fichier sur le registre du disque est enlevée. L'utilisation de programmes de récupération de données peut révéler vos mots de passes, rapports confidentiels, etc. En cas de prêt, de don, de vente ou de recyclage de votre ordinateur, il est fortement conseillé d'assurer la destruction des données personnelles et sensibles au moyen de programmes spécialement prévus à cette tâche²⁷.

²⁵ Page d'information et de démonstration : <http://www.anonymat.org/vostraces/index.php>

Chercher une adresse IP: <http://whatismyipaddress.com/>

Liste de tous les outils concernant la confidentialité : <http://epic.org/privacy/tools.html>

Camoufler son adresse IP en surfant: <http://proxify.com/>

²⁶ Pour chiffrer des données contenues sur un disque ou sur une clé USB (Windows):

<http://www.framasoft.net/article3931.html>

²⁷ Effacement de données sensibles (Windows): <http://www.framasoft.net/article1139.html>

Quelques configurations possibles avec leurs niveaux de sécurités minimums

Pour un usage quotidien

- créer ou se connecter à un compte utilisateur (différent du profil d'administrateur)
- créer ou changer le mot de passe (cf. méthode «Diceware»)
- effectuer un scan des virus et spywares
- navigateur:
 - installation les options de sécurité pour Firefox²⁸
 - contrôle des cookies (effacer les inconnus)
 - effacer l'historique de la navigation
- (vérification) sécuriser/crypter la borne Wi-Fi
- (vérification) activer le pare-feu (celui du router/modem ADSL de préférence, ou du système d'exploitation)
- courriel: ne jamais ouvrir des messages d'inconnus (virus, spywares) et ne pas donner suite au message de confirmation de compte (phishing)

Pour un usage journalistique sensible

(exemple : enquête sur un réseau terroriste ou sur la fabrication de « pipe bombs »)

- définir un nouveau compte utilisateur ad hoc (accès de visiteur, droits restreints)
- (vérification) sécuriser/crypter la borne Wi-Fi
- (vérification) activer le pare-feu (celui du router/modem ADSL de préférence, ou du système d'exploitation)
- créer un mot de passe difficile à deviner et différent de tous les autres (cf. « Diceware »)
- navigateur internet :
 - désactivation de ActiveX, java et javascript
 - installation les options de sécurité pour Firefox (cf. note de bas de page no. 22)
 - contrôle des cookies (effacer les inconnus)
 - effacer l'historique de la navigation
- **sécurisation des communications publiques** (surf sur Internet) : passer par un serveur proxy public (cf. *Guide du blogueur et du cyberdissident de RSF*²⁹)
- **sécurisation des communications privées** : cryptage des messages électroniques avec clefs privées et publiques (Comment crypter vos e-mail³⁰) ou utilisation d'un service de messagerie chiffrée (exemple : Hushmail, cf. aussi *Guide du blogueur et du cyberdissident de RSF*)
- ne jamais ouvrir des messages d'inconnus
- ne pas donner suite au message de confirmation de compte

²⁸ Navigateur Firefox: Modules de sécurité <https://addons.mozilla.org/fr/firefox/browse/type:1/cat:12>

²⁹ RSF – Guide du blogueur et du cyberdissident : http://www.rsf.org/rubrique.php3?id_rubrique=527

Comment passer outre la cybersurveillance et les mesures anti-crypto de la LSQ:

<http://www.bugbrother.com/archives/sortezcouvert.html>

³⁰ Comment crypter vos e-mails: <http://openpgp.vie-privee.org/>

Si vous êtes le nouveau «James Bond»

Dans ce cas, je vous conseille de contacter les professionnels.

Si je devais le faire sans aide externe, je me fabriquerai un outil relativement simple et très efficace: des programmes indépendants des ordinateurs stockés sur clé USB³¹, si possible avec contrôle d'accès par empreintes digitales. Muni de cet outil (bien naturellement configuré selon les règles de sécurité les plus strictes), j'utiliserais un ordinateur dans un cybercafé (avec des gants médicaux jetables qui seront brûlés). Je n'oublierais pas de payer la location en espèces sans décliner mon identité!

Grossièrement expliqué, je loue une voiture, lui enlève le moteur et le remplace par le mien pour la durée de la location. Au retour à l'agence, je démonte mon moteur et remet celui d'origine dans la voiture.

En outre, une gamme de services et de programmes plus sophistiqués³² développés par des informaticiens permettent de se soustraire à une surveillance.

Cette remarque n'exclut pas les précautions minimales de sécurité et d'anonymat proposées ci-dessus, mais il faut se rendre à une évidence:
**si une agence de renseignement ou de répression de la cybercriminalité
veut vous trouver, elle vous trouvera !**

³¹ <https://help.ubuntu.com/community/Installation/FromUSBStick>

<http://technowizah.com/2006/11/ubuntu-how-to-ubuntu-edgy-from-usb.html>

<http://www.pendrivelinux.com/2008/02/13/pendrivelinux-2008-install-from-windows/>

Produit fini achetable : http://www.dragontechnology.com/ubuntu_usb.php

Liste des programmes portables : <http://www.framakey.org/> et <http://www.pendrivelinux.com/>

Pour chiffrer des données contenues sur un disque ou sur une clé USB : <http://www.framasoft.net/article3931.html>

³² Environnement sécurisé d'échange de documents : www.martus.org

Naviguer sur la toile en détournant les contrôles : <http://psiphon.civisec.org>

Tor (permet à des journalistes de communiquer de manière plus sécurisée avec des contacts ou des dissidents) :

<http://www.torproject.org/overview.html.fr>

Comment contourner les sites bloqués : <http://www.peacefire.org/>

CONCLUSION

Les nouvelles technologies de l'information et de la communication (NTIC) font partie de notre quotidien, pour le meilleur et pour le pire. Bien que le choix de les utiliser ou non dans la sphère privée existe encore, qu'en est-il de la vie professionnelle? Force est de constater qu'elles sont devenues pratiquement incontournables.

Les défis que représentent Internet sont très particuliers. Né d'une infrastructure orpheline de parents, l'armée américaine, il est théoriquement apatride et anarchiste. Internet n'est contrôlé qu'au moyen de normes techniques (RFC - request for comment). Aucun pays ni organisme international n'a de réelle autorité, encore moins de pouvoir décisionnel ou répressif sur l'ensemble du réseau. Il n'existe pas, pour l'instant, un organisme interétatique sous la forme d'une agence de l'ONU par exemple. Cela ne veut pas dire pour autant qu'Internet échappe au contrôle des états³³. Certains pays, où les résidents vivent sous un régime de censure totale de l'information, ont établi un «nœud» d'entrée du réseau unique (Chine, Arabie Saoudite, etc.). Grâce à des arrangements particuliers avec certains moteurs de recherche (Google en Chine), ces gouvernements sont capables de filtrer 95% des recherches effectuées à partir de leur territoire.

D'autres pays plus démocratiques essaient de lutter contre les atteintes criminelles perpétrées par Internet en soumettant les fournisseurs d'accès à Internet (FAI) à de nouvelles législations tout en tentant de respecter la sphère privée. La question de la rétention par les FAI des données de connexion des utilisateurs est un bon exemple des nouvelles législations et des débats qui en résultent³⁴.

Les menaces présentées sur la toile sont un défi permanent pour les gouvernements. Elles se propagent sur une échelle planétaire à la vitesse du code binaire sur des fibres optiques, c'est-à-dire à celle de la lumière. Comment arrêter la transmission de signaux dangereux alors même que toute l'infrastructure a été pensée pour parer à une attaque à l'arme nucléaire? Les enquêtes liées à la criminalité sur Internet sont non seulement techniquement difficiles à traquer mais elles représentent un vrai casse-tête légal. La grande majorité des délits sont de natures légales différentes et relèvent de juridictions distinctes.

Comment l'utilisateur «lambda» peut-il garantir sa sécurité et son intimité dans un environnement où réseaux planétaires de cybercriminels, organisations de renseignements et services de sécurité se livrent une bataille sans merci? La réponse est peut-être trop simpliste pour être acceptable sans réserve: le respect des règles de sécurité. Afin d'éviter de subir des dommages humains et matériels, il faut être prêt à accepter certaines limitations de confort d'utilisation.

En Europe, les premières traces de la notion de vie privée datent du XVI^{ème} siècle. Ce concept a évolué au gré des courants politiques, tantôt promu par des mouvements démocratiques, tantôt mis à mal par des courants sécuritaires.

Cyberdissidence contre cyberrépression: les nouvelles technologies de l'information deviendront-elles des moyens d'émancipation ou des outils de répression?

³³ RSF - Les ennemis d'Internet: http://www.rsf.org/rubrique.php3?id_rubrique=272

³⁴ Qui obligera les FAI à filtrer les réseaux peer-to-peer:

<http://www.zdnet.fr/actualites/internet/0,39020774,39379588,00.htm>

La loi Hadopi, qu'est-ce que c'est? http://www.lexpress.fr/actualite/media-people/media/la-loi-hadopi-qu-est-ce-que-c-est_512898.html

BIBLIOGRAPHIE

Desmaretz Gérard, *Cyber-espionnage : ou comment tout le monde épie tout le monde!*, Paris : Chiron, 2007, 252 pages

Collection SVM, *Les Grands Dossier no. 2, Hors-série : Les mafias attaquent le Web*, Volnay Publications France, Puteaux, Été 2008

Moccozet Laurent, *La Présence Numérique*, Université de Neuchâtel, Faculté des lettres et des sciences humaines, Neuchâtel, Semestre de printemps 2008, 120 pages




Moccozet Laurent, *Internet : les rudiments*, Université de Neuchâtel, Faculté des lettres et des sciences humaines, Neuchâtel, Semestre de printemps 2008, 100 pages

Moccozet Laurent, *Vers le Web 2.0 et au-delà*, Université de Neuchâtel, Faculté des lettres et des sciences humaines, Neuchâtel, Semestre de printemps 2008, 326 pages

CONTROLE D'EDITION

Date :	Version :	Nom et fonction :
16 juillet 2008	1.0	Christian Brülhart, Auteur
18 juillet 2008		Laurent Moccozet, Correcteur
21 juillet 2008	1.1	Christian Brülhart, Auteur
30 juillet 2008	1.2	Christian Brülhart, Auteur

LICENCE CREATIVE COMMONS

Paternité-Pas d'Utilisation Commerciale-Pas de Modification 2.5 Suisse http://creativecommons.org/licenses/by-nc-nd/2.5/ch/deed.fr	
	Paternité. Vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre).
	Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.
	Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.