DÉPARTEMENT DES LETTRES ET COMMUNICATIONS
Faculté des lettres et sciences humaines
Université de Sherbrooke

Mémoire production

Risques technologiques et sécurité sur Internet : production d'un outil pour favoriser la prévention et fournir des pistes de solution

par
ANNIE VARIN

sous la direction de
CHANTAL-ÉDITH MASSON

présenté aux membres du jury
HÉLÈNE CAJOLET-LAGANIÈRE
et
JACQUES PIETTE

Sherbrooke
JANVIER 2011

Your file Votre référence
ISBN: 978-0-494-79801-0
Our file Notre référence
ISBN: 978-0-494-79801-0

RÉSUMÉ

Ce mémoire production vise, en premier lieu, à fournir des pistes d'explication sur la popularité et l'unicité du média Internet, pourtant jeune si on le compare aux autres grands médias traditionnels (journaux, télévision, radio). Ses caractéristiques intéressantes ont toutefois tendance à « éclipser » le risque omniprésent qui sévit sur le réseau. Les menaces sont non seulement plus nombreuses, mais aussi plus sournoises, dangereuses et potentiellement lourdes de conséquences.

Plusieurs ressources sont offertes aux utilisateurs pour les aider à se protéger sur Internet et, s'il est trop tard, pour formuler un diagnostic et obtenir une piste de solution. Quelques-unes de ces ressources, accessibles en ligne, ont été examinées pour juger de leur adéquation au besoin en protection des internautes moyens. Force était de constater qu'elles étaient souvent pertinentes, mais qu'elles présentaient également souvent des lacunes d'utilité et d'utilisabilité; or celles-ci peuvent facilement rebuter les internautes à la recherche d'information et d'aide.

Devant ce constat, il convenait, en second lieu, d'établir un cadre méthodologique pour guider l'élaboration d'un outil ergonomique pouvant être utilisé par les internautes moyens pour combler leur besoin en protection. La plateforme du site Web a été privilégiée, puisqu'elle facilite les mises à jour des contenus et des liens, un aspect essentiel pour assurer la pertinence de l'outil dans un univers virtuel en constante mutation. Ce site Web peut être consulté à l'adresse http://pages.usherbrooke.ca/securite_internet101/.

Un retour sur la production de cet outil a permis, en troisième lieu, de faire ressortir les différents obstacles rencontrés en cours de conception (lesquels ont été documentés) de même que les solutions apportées pour les surmonter.

Mots-clés : Sécurité, Internet, site Web, technologie, risque technologique, menace Internet, protection, prévention, diagnostic, solution

REMERCIEMENTS

Je tiens à remercier plusieurs personnes qui m'ont soutenue et aidée au cours de la réalisation de ce mémoire production et de l'élaboration du site Web qui lui est associé. Tout d'abord, merci à Mme Chantal-Édith Masson, ma directrice de mémoire, sans qui je n'aurai pas pu aller aussi loin. Merci pour l'inspiration, la rigueur, la réflexion, le support et l'encouragement essentiels à la concrétisation de ce mémoire. Merci également à Mme Hélène Cajolet-Laganière et à M. Jacques Piette pour leurs observations éclairées et leurs conseils. Je souhaite aussi remercier mon conjoint, ma fille et mes parents pour leur soutien inconditionnel et pour leurs encouragements tout au long de mon parcours, de même que mes collègues et patrons de Sympatico.ca pour leur flexibilité et leur appui.

Enfin, je désire remercier spécialement MM. Jacques Viau et Gabriel Hébert, anciens collègues de l'Institut de sécurité de l'information du Québec (ISIQ), pour m'avoir fait part de leurs connaissances poussées des domaines de la sécurité de l'information et de la sécurité informatique et pour m'avoir aidée à me dépasser.

TABLE DES MATIÈRES

LISTE DES ILLUSTRATIONS

LISTE DES TABLEAUX

INTRODUCTION

Au cours des deux dernières décennies, nous avons pu observer l'apparition, la croissance et l'adoption massive d'un nouveau venu dans la famille des grands médias (journaux, télévision, radio) : Internet. Même s'il est encore jeune, ce média étonne sans cesse par son dynamisme et par sa capacité à innover constamment. La vidéo en ligne, les applications Web, les contenus personnalisés et le réseautage social ne sont que quelques exemples des possibilités qu'Internet offre à ses utilisateurs. Cependant, ces avantages « alléchants » ont tendance à occulter les menaces, toujours plus nombreuses, plus subtiles et plus sévères. Elles trouvent sur Internet un milieu très favorable à leur éclosion, à leur maturation et surtout, à leur diffusion, et elles font du réseau un lieu où le risque[1] est omniprésent. Après tout, « si Internet constitue quelquefois un jardin de roses, il ne faut pas oublier qu'il comporte des épines[2] ».

Devant cette diversité et cette adversité, les internautes doivent apprendre à se protéger. Une protection efficace nécessite évidemment l'installation de logiciels de sécurité, mais également l'adoption de comportements sécuritaires, trop souvent négligés. Ces deux volets de la protection sont désormais indissociables et incontournables. Il importe donc que les internautes apprennent à développer une attitude préventive, tout en gardant à portée de main des solutions de diagnostic et de cure en cas de problèmes, car ils peuvent survenir à tout moment.

Pour obtenir de l'information, les utilisateurs disposent de nombreuses sources documentaires : livres, périodiques, sites Web, blogues, forums, groupes de nouvelles (*Usenet newsgroups*), etc. Mais ces sources peuvent parfois s'avérer décevantes à cause de faiblesses ou de lacunes aux points de vue de l'utilité (adéquation des contenus aux besoins des utilisateurs) et de l'utilisabilité[3] (intuitivité de l'interface et compréhension des explications proposées), les deux principes directeurs de l'ergonomie Web.

---

[1]Il est important de spécifier que cette mention du mot « risque » fait référence aux risques technologiques liés à l'utilisation d'Internet, ce qui inclut les menaces pouvant porter atteinte aux données confidentielles des internautes. Il n'inclut pas les risques, dangers et problèmes de nature sociale et (ou) culturelle, occasionnés en tout ou en partie par Internet (cyberdépendance, cyberintimidation, violence, pédophilie, pornographie, etc.).

[2]HUOT, François. « Discours sur l'état des menaces Internet », *Direction informatique*, vendredi 28 septembre 2007, http://www.directioninformatique.com/DI/client/fr/DirectionInformatique/Nouvelles.asp?id=45308.

[3]Dans le cadre de ce mémoire, le terme « utilisabilité » est employé pour décrire une composante de l'ergonomie Web, et non comme le synonyme d'ergonomie. De plus, le mot « utilisabilité » a été privilégié à « convivialité », puisqu'il reflète mieux le sens du mot anglais « *usability* ».

Une contribution à la réduction de cet écart entre ce qui est disponible et ce dont les internautes ont réellement besoin est au cœur du présent projet. Il s'agit donc, en une première étape de ce mémoire production, d'examiner le contexte d'Internet (poussées populaire et technologique, dimensions lucrative et réglementaire) et d'établir le portrait de ses utilisateurs de manière à bien cerner ce qui distingue Internet des autres médias et, par la suite, de définir les problèmes pouvant découler de son utilisation. Dans un second volet, il convient d'identifier les principales sources de risques, tant technologiques que comportementales, de distinguer les plus importantes menaces, d'en décrire les conséquences et d'aborder les moyens de protection. La dernière étape de la problématisation consiste à analyser un petit échantillon de ressources existantes, sélectionnées à l'aide de mots-clés « naturels »[4], pour en évaluer le degré d'utilité et d'utilisabilité pour les internautes moyens, ou *lambda*, de façon à établir et à justifier la pertinence de la présente démarche, et à délimiter le périmètre de la production.

Une telle mise en relation du contexte, de la problématique et du degré d'adéquation des ressources sert ici de base à la formulation de l'objectif, puis à la planification d'une méthodologie adaptée pour guider le développement d'un outil utile et utilisable destiné aux internautes moyens.

Enfin, un retour sur la production (hébergée en ligne) devient utile pour évaluer l'adéquation de l'outil à l'objectif. Chacune des étapes de la production (préproduction, élaboration des contenus et conception du site) est observée de plus près pour identifier ce qui a été fait, tout en mettant en lumière les difficultés rencontrées et les moyens mis en œuvre pour les régler.

Afin de faciliter la compréhension de ce document, un glossaire est disponible en annexe. La première occurrence de chaque élément du glossaire est suivie d'un astérisque (*).

[4]Les mots-clés dits « naturels » sont des mots-clés qui viennent rapidement, voire instantanément à l'esprit d'un internaute lorsqu'il effectue une recherche dans un moteur de recherche.

1. L'ÉTAT DE LA QUESTION ET L'OBJECTIF DE RECHERCHE

Avant de proposer une solution, il importe tout d'abord d'avoir une idée claire de la problématique. La sécurité des internautes va au-delà des limites d'Internet* et demande plus que des protections logicielles. Dresser un état de la question permet de comprendre la situation du média et celle de ses utilisateurs, d'observer les relations qu'ils entretiennent, d'identifier les menaces Internet les plus courantes et de saisir l'ampleur de leur portée.

Un tel portrait ne saurait être complet sans l'examen d'un échantillon de ressources existantes traitant de sécurité Internet. Les contenants et les contenus de quelques ressources sont ainsi observés afin de mettre en relief les points forts et les faiblesses, et d'évaluer leur degré d'adéquation au besoin en protection des internautes moyens. À la lumière de ces observations, il devient possible d'établir avec précision l'objectif de recherche à la base de la production de l'outil au cœur du présent projet.

1.1. L'ÉTAT DE LA QUESTION

Internet n'est pas comme les autres médias, et ce, pour plusieurs raisons : il offre un haut niveau d'interaction et de dynamisme, il permet la diffusion et le téléchargement d'une quantité presque inimaginable de contenus, il est accessible en tout temps, etc. Mais malgré ses avantages indéniables, un principal inconvénient demeure : le risque y est omniprésent.

Il est important de rappeler que cette recherche se concentre sur les risques technologiques liés à l'utilisation d'Internet, ce qui inclut la protection des données confidentielles des internautes. Les risques, dangers et problèmes de nature sociale et (ou) culturelle, occasionnés en tout ou en partie par Internet (cyberdépendance, cyberintimidation, violence, pédophilie, pornographie, etc.), ne font pas partie des sujets abordés.

1.1.1. LA SITUATION DU MÉDIA INTERNET

Depuis son déploiement « grand public » au début des années 90, Internet a pris de l'expansion d'une manière « explosive ». Les données sur le nombre d'internautes sont d'ailleurs très éloquentes : en date du 31 décembre 2009, ils étaient un peu plus de 1,8 milliard[5], une

[5] INTERNET WORLD STATS. *World Internet Usage Statistics News and World Population Stats*, 2010, http://www.internetworldstats.com/stats.htm.

augmentation de près de 400 % par rapport au nombre d'utilisateurs répertoriés en 2000, qui était d'environ 380 millions[6].

Non seulement y a-t-il plus d'internautes, mais ils passent également plus de temps en ligne. En effet, selon une étude NETendances produite par le Cefrio en 2009[7], près de 70 % des adultes québécois affirment utiliser Internet régulièrement alors qu'en 2000, ce chiffre n'était que de 39,7 %.

Mais Internet ne se démarque pas uniquement par sa popularité. Les caractéristiques uniques liées à son utilisation, ses caractéristiques techniques, les moyens qu'il offre pour générer des profits et la faible, voire inexistante, possibilité de le réglementer, lui confèrent un statut distinct parmi les médias « grand public » et ont, d'une certaine manière, contribué à son essor populaire.

1.1.1.1. LA CARACTÉRISATION DE L'UTILISATION D'INTERNET

La population internaute sans cesse croissante utilise Internet un peu comme elle le fait déjà avec les autres médias. Pourtant, certaines particularités du réseau, à savoir l'étendue de ses contenus, sa constante disponibilité et surtout, la bilatéralité des échanges qu'il permet, en commandent une utilisation différente et adaptée.

D'abord, l'**étendue** des contenus offerts sur Internet est extrêmement vaste et variée, puisque le réseau n'a, pour ainsi dire, aucune frontière et qu'il est facile de l'alimenter. La masse d'information disponible est alors beaucoup plus importante que celle offerte par les autres médias[8]. Une telle quantité de contenus renferme toutefois sa part de risque, puisque tout n'est pas de « bonne foi » sur le réseau. Par exemple, outre l'absence de crédibilité de nombreux contenus, certains sites peuvent camoufler des « pièges » publicitaires ou malveillants, d'autres peuvent servir un objectif de désinformation ou de fraude, des serveurs* peuvent proposer des fichiers infectés, etc.

Ensuite, en plus d'offrir un accès à une étendue considérable de contenus, Internet maintient son offre de manière constante, 24 heures sur 24, sept jours sur sept. Cette **disponibilité** est certes

---

[6] ZOOKNIC INTERNET INTELLIGENCE. *Internet Users*, 2008, http://www.zooknic.com/Users/index.html.

[7] CEFRIO. « NETendances – Juillet 2009 », *Blogue du Cefrio*, 2009, http://blogue.cefrio.qc.ca/2009/07/netendances-%E2%80%93-juillet-2009/.

[8] À titre indicatif, il y avait près de 207 millions de sites Web actifs sur la toile en juin 2010 (NETCRAFT. « June 2010 Web Server Survey », *Netcraft*, 2010, http://news.netcraft.com/archives/2010/06/16/june-2010-web-server-survey.html).

profitable à tous les utilisateurs qui désirent « consommer » Internet à tout moment, mais elle représente également un risque, puisqu'elle permet aux menaces d'être actives en tout temps.

Finalement, la **bilatéralité** des échanges sur Internet est une particularité cruciale, trop souvent négligée par les internautes sous son angle technique. Ce principe stipule qu'un ordinateur connecté obtient un **accès à Internet**, tout en devenant **accessible à partir d'Internet**. Or si un internaute ne tient pas compte de cet aspect, il peut ouvrir aveuglément son ordinateur au « monde virtuel », non seulement à ses « bienfaits », mais également aux « méfaits ». De plus, s'il maîtrise peu, ou pas du tout, quelques notions informatiques de base, comme le paramétrage adéquat de certains logiciels (dont le pare-feu*, le logiciel antivirus*, le navigateur*, etc.), il se met en position encore plus risquée.

1.1.1.2. LES CARACTÉRISTIQUES TECHNIQUES D'INTERNET

Internet existe grâce à un ensemble de caractéristiques techniques que la majorité des internautes ne connaissent pas. Il serait pourtant à l'avantage de tous les utilisateurs d'en savoir un peu plus sur les coulisses du réseau, ne serait-ce que pour faciliter la compréhension des principes d'étendue, de disponibilité et de bilatéralité, et des risques qui y sont associés.

Internet est un immense réseau en forme de toile. À la différence d'une structure arborescente classique, où une panne à l'un des points supérieurs (route ou nœud) entraîne automatiquement la perte d'une branche, une structure réticulaire redistribue les nœuds de sorte que si une panne survient, le réseau reste actif (donc disponible), puisqu'un autre nœud, via une autre route, aura pris la relève. Les nœuds, ce sont les **serveurs**[9], situés un peu partout dans le

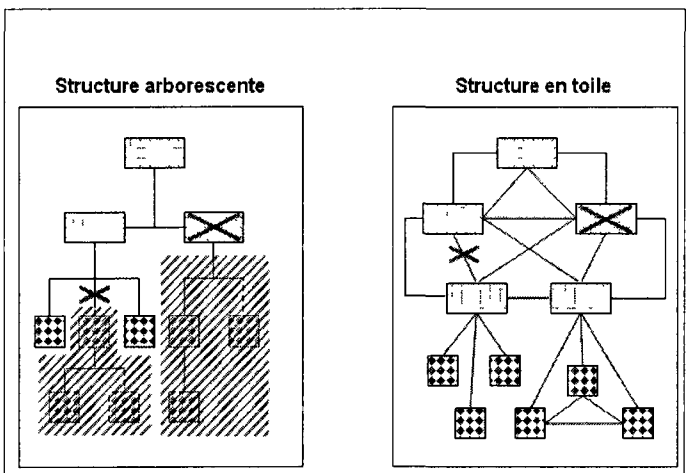


Figure 1.1 : Les structures des réseaux

[9] Il existe différents types de serveurs et ils ne remplissent pas tous les mêmes fonctions, qui ne sont d'ailleurs pas mutuellement exclusives. Il y a entre autres les serveurs de contenus (hébergeant les sites Web et autres contenus), les fournisseurs d'accès à Internet (permettant à un ordinateur client d'avoir accès au réseau) et les serveurs de routage (servant à redistribuer les données).

monde et connectés entre eux grâce à des routes sur lesquelles transite l'information (divisée en unités appelées « paquets »), et les ordinateurs **clients*** sont des ordinateurs domestiques ou de bureau, utilisés par les internautes pour se connecter à Internet.

Les différents services offerts sur Internet fonctionnent grâce à des protocoles*. Chaque protocole utilise un ou plusieurs **ports*** précis sur un ordinateur pour faire circuler des données **entre cet ordinateur et Internet**. Par exemple, le protocole HTTP*, nécessaire à l'affichage des pages Web dans un navigateur, emploie le port 80. Ces mêmes ports peuvent aussi être utilisés pour des transferts de données en sens inverse, **du réseau vers l'ordinateur**, ce qui explique la bilatéralité des échanges sur Internet. En guise d'analogie, on peut les comparer à de petites « portes » s'ouvrant et se fermant pour permettre ou limiter la circulation des données. Un faible contrôle à un ou plusieurs ports peut ainsi entraîner une fuite de données vers Internet ou une transmission de données menaçantes en provenance d'Internet.

Bien entendu, tous les protocoles ne sont pas présentés explicitement dans les applications destinées aux utilisateurs, notamment en raison de leur complexité. Après tout, les usagers n'ont pas besoin de les connaître pour utiliser Internet. Cette situation est comparable à celle d'une voiture : un automobiliste n'est pas contraint de maîtriser la mécanique automobile pour s'installer derrière le volant. De plus, il peut même choisir de ne pas entretenir son véhicule, par laxisme ou pour d'autres raisons, ce qui ne l'empêchera pas pour autant de conduire. Peu importe ses choix, il est toutefois conscient qu'une connaissance de base des mécanismes peut être d'une grande utilité en cas de problème et qu'un entretien régulier contribue au bon fonctionnement de son véhicule. Il y a là des similitudes avec ce que devrait être l'utilisation d'Internet. Dans les deux cas, l'ignorance et la négligence peuvent avoir des conséquences désagréables, voire néfastes.

1.1.1.3. LA DIMENSION LUCRATIVE D'INTERNET

Les caractéristiques uniques d'Internet quant à son fonctionnement et à son utilisation ont inévitablement contribué au développement de son grand potentiel lucratif. Cette dimension économique est d'ailleurs devenue l'un des principaux carburants de l'évolution d'Internet. Les entreprises ont exercé, et exercent toujours, une grande pression sur le développement des nouvelles technologies, qu'elles utilisent pour enregistrer des profits ou encore, pour économiser en simplifiant des processus qui, autrement, seraient plus coûteux. Force est de constater qu'elles

ont contribué à faire d'Internet un lieu unique où les nouveautés s'enchaînent et où les possibilités croissent à un rythme exponentiel. Cet univers en constante mutation est ainsi en mesure d'offrir au monde entrepreneurial des moyens toujours plus nombreux, originaux et diversifiés pour générer des profits : création de campagnes publicitaires misant sur le ciblage comportemental*, utilisation audacieuse des réseaux sociaux* pour promouvoir un produit ou un service, affichage de publicités interactives, développement d'applications Web dynamiques, etc. Pour saisir l'ampleur de ce potentiel, il est pertinent d'observer les revenus générés par la publicité en ligne[10], un domaine qui suit de près l'évolution des technologies pour offrir des produits publicitaires toujours plus innovateurs. Au Canada, en 2009, ces revenus se sont chiffré à 1,82 milliard $, ce qui correspond à 13 % des tous les revenus publicitaires canadiens générés en 2009, tous médias confondus[11]. Il s'agit d'une augmentation considérable par rapport aux recettes enregistrées en 2005, qui s'établissaient alors à 562 millions $[12].

Dans un tel contexte, les risques ne sont pas toujours évalués à leur juste valeur, ce qui peut parfois menacer les usagers. Par exemple, si une entreprise recueille des renseignements sur les utilisateurs de son site Web, elle doit en assurer la confidentialité, sans quoi ces renseignements pourraient être exposés à une potentielle exploitation malveillante. Autre exemple : lorsqu'une entreprise développe une application en ligne et qu'elle la rend accessible aux internautes, elle doit tout mettre en œuvre pour la rendre sécuritaire. Si elle ne le fait pas, les failles* de l'application sont plus à risque d'être exploitées par des individus malfaisants. Devant cette réalité empreinte de risques, les entreprises doivent se doter de mesures concrètes et efficaces pour assurer la sécurité de leurs usagers, et surtout, les internautes doivent redoubler de vigilance.

1.1.1.4. QUELQUES PRÉCISIONS TERMINOLOGIQUES

Avant d'aller plus loin, il convient de distinguer quelques termes importants et d'en décrire la nature dans le contexte de cette recherche. Une **menace** est un risque potentiel, latent et

[10]Lorsqu'il parle de publicité en ligne, le Bureau de la publicité interactive du Canada fait référence aux publicités qui s'affichent dans les résultats des moteurs de recherche (par exemple, Google), à la publicité graphique (les images, dynamiques ou statiques, présentant de la publicité à un endroit dédié dans un site), à la publicité présentée dans les sites de petites annonces, à la publicité vidéo en ligne, à la publicité par courriel et à la publicité dans l'environnement des jeux vidéo.

[11]BUREAU DE LA PUBLICITÉ INTERACTIVE DU CANADA. « La publicité en ligne au Canada atteint 1,82 milliard de dollars en 2009; et 2,1 milliards sont prévus pour 2010! », *Bureau de la publicité interactive du Canada*, 2010, http://www.iabcanada.com/newsletters/fr_081010.shtml.

[12]BUREAU DE LA PUBLICITÉ INTERACTIVE DU CANADA et ERNST & YOUNG. *2009 Actual + 2010 Estimated Canadian Online Advertising Revenue Survey*, 2010, http://www.iabcanada.com/reports/IABCanada_2009Act2010Budg_CdnOnlineAdRev_FINAL.pdf, p. 6.

omniprésent sur Internet qui peut se concrétiser en une attaque. En tant que telle, l'**attaque** est une agression informatique volontaire (en temps réel ou en différé) réalisée avec des actions ou des dispositions destinées à provoquer des sinistres[13]. Ces **sinistres** entraînent des dommages pour les ordinateurs ou leurs utilisateurs qui peuvent consister en l'altération, la destruction ou la révélation de données, la dégradation des performances d'un système, un refus de service*, l'endommagement ou le plantage* d'un ordinateur, la fraude économique, l'usurpation de fonds ou le vol d'identité*. L'attaque réussit habituellement à se concrétiser lorsqu'il y a des **vulnérabilités** (ou failles), qu'elles soient de nature humaine ou informatique (voir points 1.1.2.1 et 1.1.2.2).

Derrière les menaces se trouvent un ou plusieurs **pirates*** informatiques. Par définition, le pirate est un individu « qui parvient illégalement ou sans autorisation à accéder à un système informatique ou à une partie de celui-ci[14] ». Dans le cadre de ce mémoire, le terme « pirate » fait référence tant aux pirates « techno », usant de toutes leurs connaissances informatiques pour arriver à leurs fins[15], qu'aux escrocs utilisant Internet pour commettre des méfaits[16].

1.1.1.5. LA RÉGLEMENTATION D'INTERNET

Lorsqu'un pirate diffuse une menace sur le réseau pour éventuellement attaquer des sites, des serveurs et (ou) des internautes, et engendrer toutes sortes de dommages, il commet un acte cybercriminel*. Quelles défenses peuvent alors être opposées (en termes pénaux) aux pirates et à leurs menaces? Peut-on mettre en place un certain « contrôle » sur le réseau?

Il faut savoir que la prolifération des menaces est possible, entre autres, à cause de l'abolition des frontières, du relatif anonymat et de la quasi-absence de contrôle, des aspects qui, justement, contribuent à l'essor d'Internet et à son succès. De plus, tout « contrôle » pourrait être perçu comme une atteinte à cette « liberté » caractéristique du réseau, la frontière entre « contrôle » et

---

[13] S. GHERNOUATI-HÉLIE *Internet et sécurité*, Paris, Coll. « Que sais-je? », Paris, Presses Universitaires de France, 2002, p. 27.

[14] *Grand dictionnaire terminologique*, « Pirate informatique », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.

[15] Exemple d'une menace créée par un pirate « techno » : le développement et la diffusion d'un cheval de Troie qui, une fois installé sur un ordinateur, surveille l'internaute pour recueillir des données sensibles (numéro de carte de crédit, mots de passe, etc.) au moment où il les tape sur son clavier.

[16] Exemple d'une menace créée par un escroc utilisant Internet : un courriel en provenance d'un « héritier » d'une grosse fortune qui habite habituellement un continent lointain et qui sollicite l'aide financière d'un internaute pour « débloquer » la soi-disant fortune.

« censure » étant bien mince. Bref, si cette ouverture est si favorable aux internautes bien intentionnés, elle l'est également pour ceux dont les ambitions sont moins louables.

Le seul véritable contrôle exercé sur Internet se situe à l'échelle internationale et est d'ordre technologique, c'est-à-dire qu'il existe pour assurer l'intercommunication sur l'ensemble du réseau. Un organisme international à but non lucratif, le W3C[17], a pour tâche principale de développer et de mettre en place des « standards » (protocoles et langages*) qui servent à maintenir cette intercommunication.

La mise en place d'un contrôle supplémentaire à ce niveau serait très difficile, pour ne pas dire impossible[18]. Les seules mesures applicables concrètement relèvent des États et de leurs lois et codes, qui ne valent d'ailleurs que sur le territoire où le délit a été commis. Le caractère territorial de ces lois et codes est alors confronté à la virtualité d'Internet : la mouvance du réseau, c'est-à-dire le déplacement des données d'un serveur à un autre (à l'échelle mondiale) en cas de besoin, et le relatif anonymat possible sur Internet, viennent compliquer la tâche d'identification du lieu précis du méfait et de son auteur. Et encore faut-il qu'un individu puisse être puni pour son crime par la législation de l'État en cause, car de nombreuses disparités existent entre les États.

> En tant que rationalité, la [mondialisation] renvoie au fait que les interconnexions entre les différents réseaux emportent la création d'un espace global, à la grandeur de la planète. En ce sens, cette rationalité sous-tend l'idée que les États, entendus comme des autorités exerçant un contrôle sur un territoire déterminé, ne sont plus en mesure de régir ce qui se passe dans cet environnement global[19].

Bref, le contexte actuel d'Internet permet aux pirates de passer, parfois facilement, au travers des mailles du « filet ».

---

[17] W3C. *World Wide Web Consortium (W3C)*, 2010, http://www.w3.org/.

[18] Fait à noter, un pays peut mettre en place différents moyens pour « contrôler » Internet à l'intérieur de ses frontières (bloquer l'accès à certains sites, censurer, etc.). Outre le fait qu'une telle mesure est largement contestée à l'international, il faut se rappeler qu'elle ne garantit pas un contrôle absolu. Internet est un réseau virtuel mondial où les frontières physiques ne sont pas aussi bien définies que dans le monde « réel ». Par exemple, un utilisateur habile peut réussir à contourner les limites imposées en laissant croire au réseau qu'il se connecte à partir d'un ordinateur situé dans un autre pays.

[19] SCHILLER, D. et R.L. FREGOSO. « A Prive View of the Digital World », *Beyond National Sovereignty: International Communication in the 1990's*, 1993, p. 210-234, tel que rapporté par Yasmine EL JAMAÏ, p. 12.

1.1.2. LA SITUATION DES INTERNAUTES

Le point étant fait sur les caractéristiques particulières d'Internet, il convient maintenant de s'attarder aux internautes. L'utilisation d'Internet et du Web*[20] peut demander l'installation de nombreux logiciels et plugiciels*, du « code » pouvant comporter des failles et qui peut donc se prêter à des manipulations douteuses, voire dangereuses. Or aux côtés de ces faiblesses technologiques, se trouvent les faiblesses humaines, soit les comportements et les activités mêmes des internautes qui contribuent à les rendre vulnérables.

Il est important de rappeler que cette recherche se concentre sur les risques technologiques liés à l'utilisation d'Internet, ce qui inclut la protection des données confidentielles des internautes. Les risques, dangers et problèmes de nature sociale et (ou) culturelle, occasionnés en tout ou en partie par Internet (cyberdépendance, cyberintimidation, violence, pédophilie, pornographie, etc.), ne font pas partie des sujets abordés.

1.1.2.1. LES RISQUES LIÉS AUX LOGICIELS ET AUX PLUGICIELS

Selon les données recueillies en juin 2010 par *NetMarketShare*[21], la grande majorité des internautes (91,46 %) utilise un ordinateur PC* muni d'un système d'exploitation* Microsoft Windows (toutes versions confondues). La majorité d'entre eux (60,32 %) utilise le navigateur Internet Explorer, tandis que 23,81 % préfèrent emprunter Mozilla Firefox. D'autres navigateurs viennent ensuite récolter quelques points : Google Chrome (7,24 %), Safari (4,85 %) et Opera (2,27 %). Il va sans dire que ces pourcentages illustrent clairement la préférence des utilisateurs pour les logiciels de Microsoft, ce qui en fait des logiciels très populaires.

Il serait logique de croire qu'un logiciel (ou un plugiciel) fort populaire, issu d'une entreprise informatique connue et prospère, ne devrait présenter que peu ou pas de vulnérabilités. Malheureusement, ce n'est pas nécessairement le cas. Les fournisseurs de logiciels et de plugiciels populaires (dont Microsoft et Adobe) doivent constamment développer de nouvelles

---

[20] Il convient de distinguer « Internet » et le « Web ». Internet est comme un moteur qui fait fonctionner des services offrant des activités prisées aux internautes : navigation sur le Web, utilisation d'un service de courriel, discussion par messagerie instantanée, etc. Toutes ces activités sont recouvertes par l'étiquette « Internet »; lorsqu'on parle du Web, il s'agit d'une activité précise exécutée avec un navigateur.

[21] NET MARKET SHARE. *Market Share for browsers, operating systems and search engines*, 2010, http://marketshare.hitslink.com/.
Net Applications (la compagnie derrière *Net Market Share*) recueille des statistiques auprès d'un réseau de sites utilisant ses services. Toutes les statistiques ainsi recueillies sont compilées mensuellement et représentent un échantillon d'environ 160 millions d'internautes localisés un peu partout dans le monde.

applications toujours plus performantes et complexes s'ils désirent fidéliser leur clientèle, de plus en plus exigeante, ou capter l'attention de nouveaux utilisateurs. Ainsi, le développement des applications se trouve soumis à ce qu'on pourrait qualifier de « dictature du marketing », et un lancement prématuré peut aisément déboucher sur des erreurs ou des défaillances dans la programmation, qui se traduisent par des failles, parfois graves.

Les applications moins populaires ne sont cependant pas exemptes de vulnérabilités, puisqu'aucun logiciel ni plugiciel, peu importe son contexte de développement, n'en est à l'abri. Toutefois, leur faible utilisation dans la population internaute limite leur intérêt pour les pirates, car ces derniers cherchent souvent à profiter d'une faille présente dans un logiciel utilisé massivement, ce qui augmente le bassin de victimes potentielles. De plus, toujours en raison de leur faible rayonnement, ces applications sont moins soumises aux contraintes du marketing. Il est donc possible d'avancer qu'elles bénéficient de plus de temps pour le développement, ce qui peut se traduire par un plus faible nombre de failles, ou par un apport plus rapide de rustines de sécurité* (ou correctif de sécurité).

Par conséquent, plus un logiciel ou un plugiciel est populaire et surtout, répandu, plus il risque d'être la cible de menaces qui exploiteront ses vulnérabilités, raison pour laquelle les produits de Microsoft sont largement visés. À titre d'exemple, selon l'institut américain SANS[22], l'un des logiciels les plus attaqués (et les plus populaires) est le navigateur Internet Explorer. Certaines de ses vulnérabilités permettent même d'atteindre le système d'exploitation Windows, ce qui est possible en raison de l'« incrustation » du navigateur dans plusieurs paramètres du système d'exploitation. Ainsi, si un pirate arrive à infiltrer le système d'exploitation par une faille du navigateur, il pourrait prendre le contrôle de l'ordinateur ou accéder à des fichiers contenant des données sensibles.

1.1.2.2. LES RISQUES LIÉS AUX USAGERS ET À LEURS COMPORTEMENTS

Comme nous venons de le voir, une part importante de la sécurité sur Internet relève d'aspects technologiques, mais les comportements généraux des internautes et ce qu'ils font en ligne peuvent avoir des conséquences néfastes. En effet, la meilleure sécurité logicielle peut être compromise par des comportements inappropriés et les plus risqués sont ceux qui sont « naïfs ».

[22] SANS INSTITUTE. « SANS INSTITUTE – SANS Top-20 Security Risks (2007 Annual Update), *SANS Institute*, 2007, http://www.sans.org/top20/2007/.

Il y a d'abord la naïveté dite « technologique », où un utilisateur fait fi des aspects technologiques du réseau, dont le principe de bilatéralité. Par exemple, pensons au cas d'un internaute qui navigue sur des sites pornographiques[23], se croyant à l'abri de toute atteinte derrière son écran. Lors d'une visite sur un site en particulier, un espiogiciel* se télécharge sur son ordinateur, à son insu, et cherche des renseignements pertinents, par exemple une adresse courriel ou l'historique de navigation*. Quelques heures plus tard, l'internaute en question reçoit une dizaine de pourriels* à caractère pornographique. Il remarque également qu'une quantité impressionnante de fenêtres pop-up*, présentant des publicités liées au site douteux qu'il croyait visiter en toute impunité, s'affichent dès qu'il se connecte à Internet.

Il y a ensuite la naïveté « humaine », où un utilisateur se fait rapidement manipuler par un autre individu par le biais d'Internet. Prenons l'exemple d'un internaute qui reçoit un courriel d'une charmante inconnue (photo à l'appui) lui demandant de lui envoyer de l'argent pour qu'elle puisse venir le rencontrer et combler ses désirs. Si l'internaute transfère le montant demandé, seules ses illusions seront assouvies, car la personne derrière cette arnaque aura réussi à accomplir son vol.

Il va sans dire que plusieurs attaques sont plus subtiles et trompeuses que celles évoquées dans les exemples ci-haut. Mais peu importe la situation, croire qu'on peut accéder à tout et tout faire sur Internet en tout impunité relève de la « pensée magique », qu'elle trouve sa source dans le laxisme ou dans la « candeur ». Une utilisation d'Internet fondée sur la gratification sans réflexion ni vérification, et calquée à tort sur la consultation des médias non bilatéraux, est inappropriée et donc, risquée.

Cette réalité est d'autant plus concrète aujourd'hui avec la popularité des réseaux sociaux, qui incitent les internautes à publier de plus en plus de renseignements à leur sujet. Cette action, d'apparence anodine, est pourtant risquée. Chaque utilisateur doit savoir que dès qu'il lance une information (texte, photo, fichier vidéo, etc.) sur Internet, il lui est **impossible** d'en garder le contrôle. L'information est alors à la portée d'autres individus, étrangers ou non, qui peuvent l'utiliser, la manipuler ou la transformer à leur guise, à bon ou à mauvais escient. Et plus

[23]Les sites à caractère pornographique sont ici cités en exemple, car ces sites sont reconnus pour utiliser des moyens agressifs pour assurer leur promotion, puisqu'il leur est impossible de bénéficier d'une plateforme publicitaire « conventionnelle » en raison de la nature de leurs contenus (Réseau Éducation-Médias, « Connaître les dangers - Pornographie », http://www.media-awareness.ca/francais/enseignants/toile_enseignants/toute_securite_enseignants/dangers_pornographie.cfm).

l'utilisateur publie une grande quantité d'informations, plus il est à risque de subir les contrecoups d'une manipulation malveillante et peut-être, d'être victime d'une attaque (par exemple, d'un vol d'identité).

1.1.3. LES MENACES SUR INTERNET

« [U]n ordinateur équipé d'un système d'exploitation pour le grand public, connecté à [...] Internet et dépourvu de protection [...] est exposé à un risque de contamination [par un ou plusieurs logiciels malveillants] qui atteint 40 % au bout de dix minutes, 95 % au bout d'une heure[24]. » Ces statistiques rapportées par Sophos, compagnie œuvrant dans le domaine de la sécurité Internet (majoritairement pour les entreprises), reflètent bien l'ampleur de l'action des menaces sur Internet. Mais de quoi les internautes doivent-ils se protéger plus précisément?

1.1.3.1. LES LOGICIELS MALVEILLANTS

Avant d'aller plus loin au sujet des logiciels malveillants, il est important de mentionner que depuis 2005, il est de plus en plus question de « logiciels malveillants » plutôt que de « virus* ». En effet, le terme « logiciel malveillant » est plus englobant et plus représentatif de la diversité des menaces actuelles. Cet ajustement terminologique est également consécutif à l'arrivée massive, autour de 2005, de « nouvelles espèces » dont les espiogiciels, les logiciels publicitaires* et d'autres codes informatiques furtifs comme les vers informatiques*.

Par définition, un logiciel malveillant est un programme conçu pour être « implanté dans un système avec l'intention d'y accéder sans autorisation et d'en perturber le fonctionnement ou d'en altérer ou en dérober des données[25] ». En plus des espiogiciels, logiciels publicitaires, vers informatiques et virus, on trouve dans cette catégorie les chevaux de Troie*, les faux logiciels de sécurité* et les trousses administrateur pirate*, aussi appelées *rootkits*.

Tous confondus, les logiciels malveillants sont nombreux. Les pirates développent régulièrement de nouvelles variantes* aux programmes malicieux existants, ce qui accroît considérablement (et rapidement) le nombre total de parasites actifs sur Internet. Selon le rapport de Microsoft sur les données de sécurité[26] couvrant la période de juillet à décembre 2009, le nombre de détections de

[24] BOLCH, L. et C. WOLFHUGEL. *Sécurité informatique : Principes et méthodes*, Paris, Groupe Eyrolles, 2006, p. 68.

[25] *Grand dictionnaire terminologique*, « Programme malveillant », http://www.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp.

[26] MICROSOFT CORPORATION. *Rapport Microsoft sur les données de sécurité – volume 8 (juillet – décembre 2009)*, 2010, http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=2c4938a0-4d64-4c65-b951-754f4d1af0b5, p. 6. Ces données sont recueillies par les produits de sécurité de Microsoft, avec le consentement des utilisateurs. Elles proviennent de plus de 500 millions d'ordinateurs dans le monde et de divers services en ligne.

logiciels malveillants, tous genres confondus, a augmenté de 8,9 % en six mois seulement. Et pour le seul cas des espiogiciels, le nombre de détections a « explosé » avec une augmentation de 151,6 % en six mois.

1.1.3.2. LES AUTRES TYPES DE FRAUDES ET TROMPERIES

Les menaces ne sont pas toutes logicielles; il y a aussi les fraudes et autres tromperies qui, dans le contexte du présent projet, sont des arnaques commises par l'intermédiaire d'Internet. Certaines d'entre elles peuvent être de réelles nuisances, comme le canular* et le pourriel, et d'autres peuvent représenter un risque, parfois sérieux, pour les renseignements confidentiels des internautes, comme le témoin traceur*, l'hameçonnage* et le *pharming**.

Ces menaces sont basées sur un concept voulant que « [l]'humain [soit] la plus grosse faille de toute infrastructure informatique[27] ». Pour arriver à exploiter cette brèche, elles emploient souvent une technique d'attaque particulière et très subtile : la fraude psychologique*, communément appelée « ingénierie sociale »[28]. Il s'agit d'un ensemble de moyens utilisés pour tromper et manipuler un individu afin de l'inciter à commettre des actions ou à remettre de l'information confidentielle, tout ça dans le but de s'introduire frauduleusement dans un système, qu'il s'agisse du réseau informatique d'une entreprise ou du compte bancaire d'un individu.

1.1.3.3. LES CONSÉQUENCES ET LA PROTECTION

Les conséquences des menaces sur Internet, peu importe leur type, sont à gravité variable. Nuisance, dysfonctionnement, plantage, perte financière ou vol d'identité, tout peut arriver à un internaute « crédule », peu informé et dont le système est vulnérable.

De telles conséquences font (ou devraient faire) naître un **besoin** chez les utilisateurs, celui de se protéger lorsqu'ils sont connectés à Internet. Pour combler ce besoin, ils peuvent installer une série de logiciels de sécurité. Il s'agit toutefois d'une protection de base, car aucun logiciel, ni combinaison de logiciels, ne peut garantir la sécurité d'un ordinateur et de son utilisateur à 100 %. Plusieurs raisons expliquent ce fait, dont le comportement de l'utilisateur concerné qui, comme on l'a vu précédemment, peut compromettre, même sérieusement, la sécurité en place.

---

[27] BEAVER, K. *Combattre les hackers pour les nuls*, Coll. « Pour les nuls », Paris, Éditions First Interactive, 2004, p. 7.

[28] Fait à noter, la fraude psychologique n'est pas exclusive à Internet. Elle peut en effet être utilisée par un individu malveillant désirant commettre une arnaque en personne, par téléphone, par courrier, etc.

Les internautes à la recherche de protection doivent donc développer une attitude préventive, voire proactive, tout en gardant à portée de main des solutions de diagnostic et de cure, en cas de problème.

1.1.3.4. LA PRÉVENTION

Quand on parle de prévention, cela suppose le respect de certaines règles de base lors de l'utilisation d'Internet. Ces règles, malheureusement, sont de plus en plus complexes, puisqu'elles évoluent au rythme de l'informatique et du Web. Il y a quelque temps, à l'époque où seuls les virus et quelques autres « bestioles » marginales sévissaient, il s'agissait de ne pas ouvrir les pièces jointes suspectes, d'installer un logiciel antivirus et de le mettre à jour. Ces indications, quoique toujours valables, ne suffisent plus désormais; plusieurs précautions humaines et logicielles se sont ajoutées à cette liste.

En termes de précautions humaines, les utilisateurs doivent savoir que **dès qu'ils sont connectés, ils sont à risque**. Ils doivent donc apprendre à **gérer** ce risque. Cette **proactivité** est indissociable des notions de responsabilisation face à **soi-même** et à **autrui**. En effet, si un internaute agit de manière irresponsable, il peut représenter un important risque non seulement pour sa propre personne, mais aussi pour tous ses contacts sur Internet. Prenons le cas d'un internaute non vigilant qui a choisi d'ouvrir la pièce jointe infectée d'un courriel douteux. Ce faisant, il a exécuté un ver informatique qui, en plus de causer des dommages sur l'ordinateur contaminé, s'est automatiquement dupliqué et s'est envoyé à tous les contacts qu'il a pu trouver. Ces personnes sont alors à risque de subir les mêmes dommages et de reproduire la même erreur.

La prévention humaine ne suffit toutefois pas. Chaque ordinateur connecté à Internet doit **absolument** posséder une bonne protection logicielle, ce qui implique l'installation d'une gamme de programmes de sécurité. Les trois incontournables sont maintenant l'antivirus et l'antiespiogiciel*, dont les signatures d'infection* sont régulièrement mises à jour, ainsi que le pare-feu, correctement paramétré.

La protection logicielle ne se limite pas qu'aux programmes de sécurité; elle passe également par le choix des différents logiciels installés (système d'exploitation, navigateur, logiciel de courriel*, logiciel de traitement de texte, etc.). En effet, on se souvient que les programmes les plus populaires sont les plus attaqués. Leurs vulnérabilités sont alors plus sujettes à être

exploitées, ce qui peut compromettre, parfois sérieusement, la sécurité des ordinateurs et de leurs utilisateurs. Par conséquent, les internautes doivent installer les rustines de sécurité propres à chaque logiciel ou encore, opter pour des « logiciels de rechange* », souvent aussi puissants, sinon plus, et moins populaires.

1.1.3.5. LE DIAGNOSTIC ET LA CURE

Parfois, il arrive que même si des dispositions préventives ont été prises, elles ne soient pas suffisantes pour parer toutes les attaques. Les internautes doivent donc être en mesure d'obtenir de l'**aide**. Ils doivent bien entendu avoir accès à des ressources curatives, mais ils doivent surtout être appuyés dans leur processus de diagnostic, c'est-à-dire lors de l'identification de la menace qui les afflige. Les logiciels de sécurité peuvent fournir un diagnostic adéquat, mais ils ne sont pas une panacée; certaines menaces arrivent à déjouer leurs « mécanismes » de protection, ce qui complique ou empêche la procédure de diagnostic.

Il existe une panoplie de logiciels curatifs : gratuits, payants, avec ou sans protections supplémentaires, etc. Les internautes moyens peuvent avoir de la difficulté à trouver ce qui leur convient parmi tous les produits offerts. Mais peu importe le logiciel choisi, pour qu'ils permettent la « guérison » souhaitée, encore faut-il que le diagnostic soit le bon. Par exemple, si un virus a contaminé un ordinateur, il ne pourra pas être éradiqué par un logiciel antiespiogiciel. Et même, une fois le diagnostic établi, il est possible que la cure ne requière aucun logiciel, par exemple dans le cas d'une attaque par hameçonnage, où l'internaute doit, en plus d'assurer sa protection logicielle, contacter des organismes s'il souhaite obtenir de l'aide.

1.1.4. LES RESSOURCES DISPONIBLES, LEUR EFFICACITÉ ET LEURS LIMITES

En principe, les internautes ne sont pas démunis lorsqu'ils cherchent à combler leur besoin en protection. Ils ont accès à des ressources (ouvrages, sites Web, etc.) sur la prévention des dégâts ou, s'il est trop tard, sur la mise en œuvre de solutions adéquates. Pourtant, dans bien des cas, la consultation de ces ressource n'est pas aisée, et ce, pour diverses raisons : contenus peu vulgarisés, interface difficile à manipuler (dans le cas d'un site Web), etc.

Bref, même lorsqu'ils désirent obtenir de l'information et s'investissent en ce sens, ils n'arrivent pas toujours à s'y retrouver. Un examen de quelques ressources disponibles s'est alors avéré pertinent afin de comprendre pourquoi.

1.1.4.1. L'ÉCHANTILLON

Puisque le site Web est le support choisi pour la production de l'outil au cœur du présent projet (voir l'objectif du projet au point 1.2), l'échantillon de cet examen[29] ne comprenait que de sites Web. Cette observation était destinée à évaluer si, et dans quelles mesures, les ressources courantes offertes en ligne combinaient les renseignements nécessaires pour combler le besoin en protection des internautes moyens (précédemment identifié au point 1.1.3.3), et si elles étaient aisément manipulables.

Il ne s'agissait pas donc pas de faire un recensement, mais bien de choisir un échantillon caractéristique de sites Web **francophones**, traitant de **sécurité Internet**, et destinés en tout, ou en partie, à fournir de la documentation et de l'aide aux **internautes moyens**.

Une fois ces conditions préalables établies, une recherche en ligne a été entamée pour repérer des sites pertinents. En premier lieu, une requête composée des descripteurs francophones « Sécurité Internet » a été lancée sur le moteur de recherche Google[30]. Ces descripteurs, pourtant simples, peuvent venir « naturellement » à l'esprit d'un internaute moyen, raison pour laquelle ils ont été choisis. Une fois la recherche complétée, le nombre de résultats s'est élevé à plus de 26 millions.

En second lieu, les sites résultants ont été sommairement filtrés en suivant leur ordre d'apparition dans les résultats de Google, lequel tient compte entre autres de la fréquence de consultation. Seuls les cent premiers ont été consultés.

En troisième lieu, de ces cent sites, certains ont été exclus, car il s'agissait de :

- sites personnels : il était difficile d'en juger la fiabilité;
- sites d'entreprises : ils concentraient souvent l'information sur la vente d'un produit;
- sites traitant majoritairement de l'actualité technologique (par exemple, Technaute – http://technaute.cyberpresse.ca/) et les blogues (par exemple, Synchro Blogue – http://www.synchro-blogue.com/) : l'information changeait trop souvent et les sujets n'étaient pas toujours traités en profondeur;

[29]Cet examen a été effectué pour la première fois en décembre 2007. Il a subi plusieurs mises à jour par la suite. La dernière mise à jour s'est tenue le 26 juin 2010.

[30] Google est utilisé par près de 85 % de la communauté internaute (NET MARKET SHARE. *Market Share for browsers, operating systems and search engines*, juin 2010, http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=4), raison pour laquelle il est le moteur de recherche employé dans cet examen.

- sites de surveillance des menaces : l'information y était très technique et peu accessible.

En parallèle à cette recherche, les connaissances techniques de l'étudiante[31] ont été mises à profit pour repérer d'autres sites pertinents.

Ensuite, les sites retenus à la fin de cette première étape ont été validés auprès d'un réseau de références crédibles et actuelles afin d'en assurer la **fiabilité**. Ce réseau était composé de différents experts de la sécurité actifs dans les forums* sur le sujet[32], et de deux spécialistes de la sécurité de l'information et la sécurité informatique consultés de vive voix à l'Institut de sécurité de l'information du Québec (ISIQ)[33].

Finalement, une observation sommaire des deux grands critères de l'ergonomie Web*, soit l'**utilité*** (Est-ce que le site répond au besoin en protection et aux attentes des internautes moyens? Est-ce qu'il est crédible?) et l'**utilisabilité*** (Est-ce que les contenus sont aisément atteignables, ce qui suppose que l'interface est facilement manipulable? Est-ce que les contenus peuvent être décodés facilement?) a été effectuée pour ne retenir que les sites qui semblaient accessibles aux utilisateurs moyens.

Au terme de ce repérage, quatre sites[34], dont l'importance est d'ailleurs attestée sur la base des références présentes sur de nombreux sites ayant « pignon sur rue » dans le domaine de la sécurité, ont été retenus. Des saisies d'écran* des pages d'accueil de ces quatre sites se trouvent à l'annexe 2.

- Secuser.com (http://www.secuser.com);
- Internet 101 (http://www.internet101.ca)[35];
- Assiste (http://www.assiste.com);

[31] L'étudiante possède une bonne expérience dans le domaine des technologies, puisqu'elle a travaillé dans le domaine de la sécurité de l'information et a enseigné le multimédia à l'université et dans différentes écoles technologiques de formation continue.

[32] Entre autres sur le forum informatique de Commentçamarche.net (http://www.commentcamarche.net/forum/virus-securite-7)

[33] INSTITUT DE SÉCURITÉ DE L'INFORMATION DU QUÉBEC (ISIQ). *ISIQ*, 2009, http://www.isiq.ca/.

[34] Les sites Techno.branchez-vous.com, 01Net.com, Vulgarisation-informatique.com et Protegetonordi.com, retenus dans le projet de recherche précédant ce mémoire, ont dû être retirés de l'examen dans le cadre d'une mise à jour des observations effectuée le 26 juin 2010. Le site Techno.branchez-vous.com a abandonné la section sur la sécurité Internet au profit des actualités et des blogues, le site 01Net.com a réorienté les rubriques sur la sécurité Internet vers la vente de logiciels de sécurité, le site Vulgarisation-informatique.com a pris une tangente logicielle et technique qui amenuisait sont utilité dans cet examen et le site Protegetonordi.com n'existe plus (l'adresse URL est toujours utilisée, mais le site de référence n'est plus).

[35] Le site Internet 101 observé dans le cadre de cet examen n'est plus accessible en ligne.

- Le portail de la sécurité informatique (http://www.securite-informatique.gouv.fr).

1.1.4.2. L'EXAMEN DE L'ÉCHANTILLON

Chaque site sélectionné a fait l'objet d'un **examen plus approfondi** sous l'angle de l'**utilité** et de l'**utilisabilité** afin de mettre en relief les points forts et les faiblesses.

Les critères d'utilité correspondaient aux prérequis nécessaires pour qu'un site puisse être « adapté aux besoins et attentes de l'utilisateur[36] ». Les critères ergonomiques de Domique Scapin et Christian Bastien[37] (détaillés au point 2.3) ont permis d'établir les critères d'utilisabilité, qui étaient en plus appuyés par les recommandations de l'ouvrage *De la lettre à la page Web : Savoir communiquer avec le grand public*[38] du Gouvernement du Québec relatives à la maniabilité des sites Web.

- **Utilité du site (pertinence)**
  - **Crédibilité du site :** la crédibilité est étroitement liée aux entités (propriétaires, collaborateurs, auteurs, etc.) qui ont permis la création du site et qui participent à la pertinence de ses contenus. Pour être considéré comme crédible, chaque site observé devait faire affaire avec des entités reconnues et surtout, fiables.
  - **Récence des contenus :** pour juger de la récence des contenus, un aspect vital compte tenu de la vitesse à laquelle se développent les menaces et leurs nouvelles variantes, une date devait d'abord être inscrite pour permettre aux internautes de savoir si ce qu'ils consultaient était d'actualité ou non. Ensuite, puisque le temps est accéléré sur la toile, tout contenu abordant la sécurité Internet qui n'avait pas été mis à jour récemment (au cours des deux dernières années) était considéré comme désuet.
  - **Complétude des contenus sur la sécurité Internet :** pour être considérés comme « complets », les contenus devaient fournir de l'information sur les menaces, en plus de traiter de la prévention, du diagnostic à effectuer et de la cure à entreprendre en cas d'infection.

---

[36] *Grand dictionnaire terminologique*, « Ergonomie Web », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.

[37] « Les critères ergonomiques de Scapin & Bastien, Partie 1 – Ergolab », *Ergolab, ergonomie Web et logiciel*, http://www.ergolab.net/articles/criteres-ergonomiques-1.php.

[38] CLERC, I. et É. KAVANAGH – GOUVERNEMENT DU QUÉBEC. *De la lettre à la page Web : Savoir comment communiquer avec le grand public*, 376 p.

- **Utilisabilité du site (interface et navigation)**
    - **Menus :** les menus sont à la base de la navigation et leur manipulation doit être simple, sans quoi les internautes ne sont pas portés à circuler dans le site et ainsi, à « approfondir » leur visite. Les menus devaient être clairs, leurs étiquettes, univoques, et ils devaient être peu chargés.
    - **Hyperliens :** un seul site peut donner différentes apparences à ses hyperliens (certains peuvent être soulignés, d'autres peuvent changer de couleur, etc.). Lors de cet examen, **tous** les hyperliens devaient être aisément repérables, peu importe leur apparence.
    - **Aides à la navigation* :** pour trouver ce qu'ils cherchent, les internautes devaient pouvoir obtenir de l'aide avec des aides à la navigation (champ de recherche, plan du site, index ou sommaire). Ces derniers devaient être présents et facilement repérables.
    - **Repères de position :** lorsqu'un internaute est perdu dans un site, il doit être en mesure de savoir où il se trouve. Pour ce faire, il peut observer des repères de position comme un titre de page explicite ou un fil d'Ariane*. Au moins un de ces repères devait être présent et aisément repérable.
    - **Interface soignée, épurée et constante :** la simplicité de l'interface facilite la navigation des utilisateurs tout en agrémentant leur expérience. À l'inverse, une interface trop chargée de texte, d'hyperliens et parfois de publicités, peut « embrouiller » les internautes et saturer leur capacité à traiter l'information. Les interfaces observées devaient respecter ces critères de simplicité.
- **Utilisabilité des contenus (lisibilité, accessibilité, adaptation et vulgarisation)**
    - **Densité :** pour être utilisable, un contenu ne doit être ni trop dense, car il peut décourager même les internautes les plus hardis, ni trop léger, car il perd alors en utilité. Les contenus observés devaient présenter une densité adéquate, c'est-à-dire que les paragraphes devaient être courts et l'emploi de listes à puces et de sous-titres devait être privilégié pour « aérer » le texte.
    - **Contenus adaptés et vulgarisés :** les internautes moyens doivent comprendre ce qu'ils consultent. Par conséquent, les contenus devaient être faibles en jargon

technologique, ou définir de manière claire et précise les termes complexes de façon abordable lorsque nécessaire.

- **Utilisation d'exemples :** toujours dans une optique de vulgarisation, si une notion ou un terme technologique était employé sans aucune adaptation, il devait être exemplifié.
- **Utilisation de compléments graphiques pertinents :** les compléments graphiques (images, graphiques, saisies d'écran, etc.) apportent une grande contribution à la vulgarisation d'un contenu. Leur présence, leur utilisation et leur pertinence ont été observées.

1.1.4.3. LES RÉSULTATS DE L'EXAMEN

Les résultats de ce bref examen montrent que, malgré le fait que les sites Web repérés traitaient tous sensiblement du même sujet, chacun d'eux n'avait pas les mêmes forces. Et encore là, ce qui était le point fort de l'un pouvait aisément devenir le point faible de l'autre.

L'utilité du site

Tableau 1.1 : L'utilité du site

		Secuser.com	Internet 101	Assiste	Portail de la sécurité informatique
Utilité du site	Crédibilité du site (propriétaire reconnu, collaborateurs fiables)	x	x	x	x
	Récence attestée des contenus				x
	Complétude des contenus sur la sécurité Internet (information, prévention, diagnostic et cure)	x	x	x	x

Au point de vue crédibilité, tous les sites ont fait bonne figure, mais à différents degrés. Par exemple, des acteurs aussi influents que la Gendarmerie royale du Canada (GRC) et la Sûreté du Québec (SQ, district de l'Outaouais) faisaient partie des partenaires fondateurs du site Internet 101. Chez Assiste, l'auteur et propriétaire du site s'affichait comme consultant en sécurité informatique et en protection de la vie privée auprès des particuliers, des institutions et des

commerces, ce qui lui conférait, à première vue, une certaine crédibilité, quoique limitée. Dans le cadre d'une recherche plus approfondie, il serait intéressant d'en savoir plus sur l'expérience de cet auteur et propriétaire pour évaluer sa crédibilité de manière plus pointue.

En ce qui concerne la récence des contenus, deux constats ont fait surface : peu de sites ont daté leurs pages et si des dates étaient inscrites, elles révélaient l'âge réel (et la potentielle désuétude) des contenus. Par exemple, le site Internet 101 n'avait inscrit aucune date. Chez Secuser.com, il y avait des rubriques datant de 2000, ce qui est considéré comme « archaïque » dans le domaine informatique. Ces contenus de Secuser.com étaient certes intéressants dans leur ensemble, mais ils méritaient une importante mise à jour pour être jugés utiles.

Finalement, du côté de la complétude des contenus, la plupart des sites offraient de l'information sur les menaces. Cependant, en ce qui concerne la prévention, le diagnostic et la cure, quelques sites n'exploraient pas suffisamment le sujet en profondeur. Par exemple, Internet 101 misait abondamment sur la prévention et effleurait le sujet de la cure, mais ne fournissait aucun renseignement sur le diagnostic. Ce n'était pas une lacune en soi, puisque l'objectif du site était de traiter de prévention. Cependant, dans le cadre de cet examen, il devenait moins utile compte tenu du besoin en protection des internautes moyens, au cœur de la présente démarche.

L'utilisabilité du site

Tableau 1.2 : L'utilisabilité du site

		Secuser.com	Internet 101	Assiste	Portail de la sécurité informatique
Utilisabilité du site	Menus clairs courts, aux étiquettes univoques, et peu chargés		x		x
	Hyperliens **tous** facilement repérables	x		x	
	Aides à la navigation facilement repérables		x		
	Repères de position clairs		x	x	x

L'emploi d'un menu simple (étiquettes claires, faciles à comprendre) et concis (menu comprenant un nombre peu élevé d'éléments cliquables) ne semblait pas faire loi parmi les sites observés. La principale lacune des menus était leur teneur, c'est-à-dire la quantité d'éléments cliquables qu'ils contenaient; bien souvent, ces éléments étaient trop nombreux. Par exemple, le site Secuser.com comportait un menu de gauche beaucoup trop chargé[39]. Dans le site Assiste[40], c'était la clarté du menu qui était remise en question; chaque élément n'était pas toujours « mutuellement exclusif », ce qui pouvait induire l'internaute en erreur. Le menu comportait entre autres les étiquettes « Outils gratuits » et « Télécharger », deux éléments similaires, mais présentés comme différents. Il était d'ailleurs difficile de déterminer sur quelles bases reposait cette différence.

Du côté des hyperliens, il y avait négligence sur certains sites. Mis à part les hyperliens du menu, ceux présents dans les contenus n'étaient pas toujours facilement repérables. Par exemple, sur le Portail de la sécurité informatique, certains hyperliens pouvaient aisément passer pour des sous-titres; pour savoir qu'ils étaient cliquables, il fallait les survoler avec le curseur. Ils n'étaient donc pas facilement repérables.

En ce qui concerne la navigation dans le site, les aides à la navigation (champ de recherche, plan du site, index ou sommaire) n'étaient pas toujours facilement accessibles. Par exemple, sur les sites Secuser.com et Assiste, le champ de recherche (seule aide à la navigation disponible) était difficile à repérer, et sur le Portail de la sécurité informatique, aucune aide à la navigation n'était offerte. Du côté des repères de position, seul le titre de page était utilisé. Par exemple, sur Internet 101, le titre était parfois suffisamment explicite pour indiquer à l'internaute où il se trouvait dans le site. Mais sur Assiste, où il était facile de se perdre en raison de la complexité du menu et de la quantité faramineuse d'hyperliens; d'autres repères de position (dont le fil d'Ariane) auraient été nécessaires.

Enfin, la plupart des interfaces des sites observés étaient soignées et épurées sauf sur Assiste, où elle était visiblement trop chargée (surtout en textes et en hyperliens). De plus, toujours sur ce site, l'interface avait parfois tendance à changer d'une page à l'autre. Ces changements n'étaient pas majeurs, mais ils pouvaient être suffisants pour « dérouter » l'internaute et l'inciter à quitter le site.

---

[39]L'annexe 2 présente une saisie d'écran de la page d'accueil du site Secuser.com.
[40]L'annexe 2 présente une saisie d'écran de la page d'accueil du site Assiste.

L'utilisabilité des contenus

Tableau 1.3 : L'utilisabilité des contenus

		Secuser.com	Internet 101	Assiste	Portail de la sécurité informatique
Utilisabilité des contenus	Densité adéquate dans l'ensemble du site	x	x		x
	Contenus vulgarisés (faible utilisation du jargon technologique vocabulaire abordable)	x	x	x	x
	Utilisation d'exemples		x	x	x
	Utilisation de compléments graphiques pertinents			x	x

Dans la plupart des sites, la densité des contenus était adéquate, puisqu'ils étaient « aérés ». L'information était divisée avec des sous-titres évocateurs et de courts paragraphes, en plus d'être synthétisée avec des listes à puces à certains endroits. Certaines pages du site Secuser.com[41] en sont un bon exemple.

Côté adaptation et vulgarisation, les sites présentaient des contenus facilement « décodables » pour les internautes moyens. Par exemple, le site Assiste employait beaucoup de comparaisons (mise en relation d'un comparant et d'un comparé pour évaluer leur ressemblance ou leur différence) et d'analogies (désigne le rapport entre des éléments qui ont des similitudes). Il présentait aussi un texte au langage familier et plus « formel » lorsque requis, en plus d'exemples et de quelques compléments graphiques évocateurs pour vulgariser tout jargon technologique (sauf dans les sections destinées aux connaisseurs) et pour expliquer des notions complexes.

En ce qui concerne plus précisément les compléments graphiques, quelques sites ne semblaient pas attribuer la même importance à leur impact. Par exemple, de bien jolies images accompagnaient les contenus sur Internet 101, mais elles ne faisaient qu'embellir l'interface, elles ne participaient pas à la vulgarisation. Même constat chez Secuser.com; les images ne servaient qu'à des fins esthétiques. À l'inverse, le Portail de la sécurité informatique employait beaucoup

[41] Voir exemple à la page http //www secuser com/dossiers/virus_generalites htm

de saisies d'écran pour expliquer des notions plus « technologiques »[42], comme le paramétrage de certains logiciels.

Constat global : liste des critères minimaux à remplir

À la lumière des résultats de l'ensemble de cet examen, on remarque qu'aucun site analysé ne semblait être en mesure de répondre parfaitement au besoin en protection des internautes moyens précédemment identifié (information sur les menaces, prévention, **et** diagnostic et cure), que ce soit à cause de faiblesses d'utilité (faible crédibilité, fiabilité boiteuse, contenus incomplets) ou d'utilisabilité (difficultés de manipulation de l'interface, incompréhension de la structure du site, accessibilité des contenus à développer), parfois majeures. Selon ces observations, le Portail de la sécurité informatique était certes le site le plus ergonomique dans l'échantillon, mais certaines lacunes d'utilisabilité affaiblissaient sa « navigabilité ».

Devant ce constat, il devient alors pertinent de mettre à la disposition des utilisateurs un outil qui rassemble les forces des sites observés et qui pallie leurs faiblesses. Ces forces et faiblesses ont été identifiées et compilées afin de produire une liste de critères que l'outil au cœur du présent projet devra respecter.

- **Utilité du site**
    - **Présenter tout élément pouvant renforcer la crédibilité du site** (partenaire, auteur renommé, etc.).
    - **Inscrire une date sur chaque page contenant du texte pour que les internautes moyens puissent juger de la récence des contenus.**
    - **Assurer la mise à jour des contenus s'ils « prennent de l'âge », pour garantir leur utilité.** Dans le cadre de ce projet, si les contenus ont plus de deux ans, ils sont considérés comme désuets.
    - **Assurer la complétude des contenus du site dans son ensemble**, c'est-à-dire présenter de l'information sur les menaces et traiter de prévention, de diagnostic et de cure.

[42] Voir exemple à la page http://www.securite-informatique.gouv.fr/gp_article140.html.

- **Utilisabilité du site**
    - **Créer des menus peu chargés** (nombre peu élevé d'éléments cliquables, autant que possible) **et aux étiquettes claires et univoques.**
    - **Rendre les hyperliens facilement repérables.** Bon nombre d'internautes sont habitués de voir des hyperliens soulignés. Il est pertinent de capitaliser sur ces connaissances acquises.
    - **Utiliser au moins une aide à la navigation**, comme un plan du site.
    - **Utiliser des repères de position clairs.** Les titres sont de bons repères de position s'ils sont clairement visibles au début d'un texte, mais le meilleur repère demeure le fil d'Ariane, car il expose le « chemin » parcouru pour atteindre une page.
    - **Créer une interface épurée.**
- **Utilisabilité des contenus**
    - **Limiter la densité des contenus.** Utiliser des sous-titres évocateurs pour diviser le texte et des listes à puces pour synthétiser certaines sections.
    - **Vulgariser et adapter le texte**. Les comparaisons et les analogies favorisent grandement la compréhension, de même que des définitions aux termes complexes.
    - **Utiliser des exemples**.
    - **Utiliser des compléments graphiques pertinents** lorsque c'est nécessaire.

1.2. L'OBJECTIF DU PROJET

Comme on a pu le constater, grâce à ses caractéristiques uniques par rapport aux autres médias, Internet est devenu, au fil du temps, très populaire. Cette popularité s'est traduite par un accroissement de la quantité de contenus, qui sont toujours plus diversifiés, dynamiques et interactifs, et qui nécessitent par conséquent une mécanique sous-jacente plus complexe. Cette sorte de « spirale inflationniste » le rend cependant encore plus « alléchant » aux yeux des utilisateurs, qui représentent une clientèle de plus en plus hétérogène et dont une bonne partie se laisse « hypnotiser » par le côté gratifiant du média.

Sous la poussée du réseau, les menaces sont non seulement plus nombreuses, mais aussi (et surtout) plus lourdes de conséquences. Il importe donc que les internautes se responsabilisent, c'est-à-dire qu'ils développement des compétences informatiques (au moins de base) et adoptent des comportements prudents.

Bien que certains internautes cherchent à s'informer de manière préventive, la majorité d'entre eux entament leurs recherches lorsque des problèmes surviennent et qu'ils ont besoin d'aide. Toutefois, pour bien se protéger, ils ne doivent pas compter seulement sur des ressources curatives; ils doivent apprendre à développer une attitude proactive, tout en gardant à portée de main différentes ressources pour établir un diagnostic et apporter une solution en cas de difficulté. Pour y arriver, ils peuvent consulter des sites Web qui sont habituellement bien intentionnés, mais qui ne conviennent pas toujours en raison de lacunes, parfois importantes, aux points de vue de l'utilité et de l'utilisabilité.

Pour pallier ce manque de ressources accessibles, ce projet a pour objectif d'instrumenter les internautes avec la production d'un **outil** leur fournissant, dans un seul et même lieu, des explications claires et abordables couvrant les menaces les plus courantes, des définitions, des outils interactifs et des ressources accessibles (logiciels, organismes à consulter, etc.), et pouvant être consulté pour obtenir de l'information et de l'aide sur la **prévention**, le **diagnostic** et la **cure**. Pour développer cet outil, le site Web est privilégié, car le meilleur moyen d'atteindre le plus grand nombre d'internautes est encore d'employer le type de média qu'eux-mêmes privilégient. Ce site, utile et utilisable, doit capitaliser sur les forces des autres sites observés lors de l'examen des ressources existantes, et pallier leurs faiblesses. L'objectif de ce projet peut alors être exprimé dans l'équation suivante :

Popularité croissante d'Internet	+	Complexité en hausse d'Internet	+	Comporte-ments des internautes	+	Quantité de menaces en hausse	−	Documentation (sites Web) compréhensible et réponses accessibles	=	Besoins à combler : outiller les internautes (prévention, diagnostic et cure)

Figure 1.2 : L'objectif du projet en équation

2. MÉTHODOLOGIE

Avant d'entamer les modalités de l'élaboration de l'outil, il convient d'abord de préciser les détails relatifs au choix du support, puis d'établir les critères essentiels d'utilité et d'utilisabilité qui doivent guider la conception. Il s'agit là des deux principales composantes de l'ergonomie Web, une discipline « qui se caractérise par l'adaptation ou la création des contenus et des fonctionnalités d'un site Web en vue d'en faciliter l'utilisation par ses visiteurs[43] ».

L'examen de quelques ressources existantes a déjà permis de dresser une liste de critères à respecter lors de la production finale (voir point 1.1.4.3). Ces critères sont en lien avec ceux énumérés dans la méthodologie, ce qui en assure le respect lors de la création de l'outil.

2.1. LE CHOIX DU SUPPORT

Un site Web est un acte de communication en soi, car il permet un transfert d'information (le message) d'un émetteur vers un destinataire (pour lequel il est adapté) en empruntant le canal Internet. Il s'agit en effet du canal le plus susceptible de rejoindre les internautes, pour des raisons évidentes. De plus, Internet, contrairement aux autres médias, se prête à une grande adaptation des contenus et des stratégies en fonction des besoins, en facilitant la mise à jour des contenus et des liens, ce qui en fait un support de choix dans le cadre de ce projet en raison, entre autres, de l'évolution constante du sujet.

2.2. L'UTILITÉ DU SITE

Un site Web est utile et de ce fait, pertinent, lorsqu'il fait ce que demande l'utilisateur[44], c'est-à-dire qu'il arrive à répondre à ses attentes. L'utilité, première composante de l'ergonomie Web, vient se placer au cœur du processus communicationnel, puisqu'elle commande l'établissement du public cible et le choix des contenus qui lui seront présentés.

2.2.1. LE PUBLIC CIBLE

Le public ciblé est celui des adultes (18 ans et plus) francophones, visés en tant que particuliers, ayant une connaissance fonctionnelle et limitée de l'informatique et possédant un ordinateur

[43] *Grand dictionnaire terminologique*, « Ergonomie Web », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.
[44] NIELSEN, Jakob. « Usability 101: Definition and Fundamentals - What, Why, How (Jakob Nielsen's Alertbox) », *Useit.com*, 2008, http://www.useit.com/alertbox/20030825.html.

personnel connecté à Internet et roulant sous le système d'exploitation Windows (parce qu'il est le plus répandu). Ces internautes sont considérés comme des utilisateurs moyens, ou *lambda*.

Bien que tous les internautes soient invités à consulter le site, il doit être d'abord conçu pour ceux qui cherchent à combler un besoin en protection (identifié au point 1.1.3.3). De plus, si les contenus dits « technologiques », notamment ceux touchant aux marches à suivre et aux suggestions logicielles, doivent refléter davantage les attentes des internautes du public cible, les contenus abordant les comportements doivent s'adresser à tous les visiteurs.

2.2.2. LES CONTENUS

Les contenus choisis portent donc sur l'identification, le tri et l'explication de la nature, du fonctionnement et des conséquences des principales menaces sur Internet. Ils portent également sur les moyens à prendre pour prévenir chaque menace identifiée (développement d'une attitude proactive, tant humaine que logicielle) et, s'il est trop tard, pour mettre en œuvre une solution.

En parallèle aux descriptions des menaces, une forme d'aide au diagnostic doit être offerte pour aider les internautes dans leur recherche d'information, qu'il s'agisse de découvrir de quelle menace ils sont affligés ou de trouver rapidement une réponse à leur question. L'important est de leur donner accès à de l'information claire et pertinente pour qu'ils puissent établir un diagnostic par eux-mêmes.

Certains éléments sont exclus des contenus, à savoir les détails techniques sur le fonctionnement d'Internet, de même que les préalables à la navigation Web (connexion à Internet, manipulation d'un navigateur, etc.), puisque le site s'adresse à des usagers qui sont en mesure d'utiliser le réseau. Il est important de rappeler que bien que l'information technologique concerne les ordinateurs roulant sous Windows, les explications portant sur les comportements demeurent valides pour tous les systèmes d'exploitation.

Pour optimiser leur utilité, les contenus doivent également être datés, sans quoi les internautes ne peuvent juger de leur récence et par conséquent, de leur validité. De plus, tout élément pouvant renforcer la crédibilité du site doit apparaître sur des pages clés telles que la page d'accueil, ce qui tend à rassurer l'utilisateur dans son choix de ressource.

2.3. L'UTILISABILITÉ DU SITE ET DES CONTENUS

En tant que telle, l'utilisabilité se définit comme une « caractéristique de qualité liée à la facilité de se servir de quelque chose[45] » et il s'agit de la deuxième composante de l'ergonomie Web. Son objectif consiste à rendre un site efficace (permettre à l'utilisateur de trouver ce qu'il cherche), efficient (faciliter la tâche d'apprentissage de l'utilisateur) et satisfaisant (agrémenter l'expérience de l'utilisateur)[46]. Pour que cet objectif soit atteint, le site doit être facilement manipulable et ses contenus, compréhensibles.

Les huit critères ergonomiques de Dominique Scapin et Christian Bastien[47] servent de repères d'utilisabilité pour l'élaboration de l'outil[48], et sont complétés par l'ouvrage *De la lettre à la page Web : Savoir communiquer avec le grand public*[49] du Gouvernement du Québec, qui traite de la maniabilité des sites Web. Il est important de spécifier que dans le cadre d'une recherche plus approfondie, une analyse complète de l'utilisabilité de ce site serait pertinente.

2.3.1. PREMIER CRITÈRE : LE GUIDAGE

Le guidage, c'est tout mettre en œuvre pour conseiller, orienter, informer et conduire l'internaute à l'intérieur du site Web. Ce critère comprend quatre sous-critères :

1. **L'incitation :** utiliser différents moyens pour que l'utilisateur comprenne le contexte du site sur lequel il se trouve et les actions qu'il peut y poser. Ces moyens incluent les repères de position (par exemple, le titre de la page et le fil d'Ariane), qui lui permettent de se situer rapidement, les aides à la navigation (par exemple, le plan du site), qui facilitent le balisage du « micromonde » que représente le site Web, et une

[45] NIELSEN, J. et H. LORANGER. *Site Web : priorité à la simplicité*, Paris, CampusPress, 2007, p. XVI.
[46] ORGANISATION MONDIALE DE NORMALISATION. « ISO 9241-11:1998 - Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) -- Partie 11: Lignes directrices relatives à l'utilisabilité », *ISO*, 1998, http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=1688.3, tel que repris par Stephanie Le Rouzic dans le site Utilisabilité.info (http://www.utilisabilite.info/dotclear/index.php?Normes).
[47] « Les critères ergonomiques de Scapin & Bastien, Partie 1 – Ergolab », *Ergolab, ergonomie Web et logiciel*, http://www.ergolab.net/articles/criteres-ergonomiques-1.php.
[48] Les critères de Scapin et Bastien ont été choisis entre autres pour leur clarté, mais également en raison de leur généralité; le fait qu'ils ne soient pas trop précis permet d'élargir le champ d'observation et ainsi, de trouver des erreurs qui, autrement, n'auraient pas fait surface (*Ergolab, ergonomie Web et logiciel*, http://www.ergolab.net/articles/criteres-ergonomiques-1.php).
[49] CLERC, I. et É. KAVANAGH – GOUVERNEMENT DU QUÉBEC. *De la lettre à la page Web : Savoir comment communiquer avec le grand public*, 376 p.

mise en forme adéquate permettant l'identification rapide et la compréhension des zones cliquables (menus et hyperliens)[50].

2. **Le groupement et la distinction :** grouper les éléments qui vont ensemble et séparer ceux qui ne vont pas ensemble. Il y a d'abord le groupement par localisation, qui vise à rassembler les éléments similaires dans un même « lieu ». Par exemple, tous les contenus traitant d'un même sujet sont regroupés dans une même section. Ce sous-critère est souvent associé au menu, qui expose les différents regroupements. Il y a également le groupement par format, qui commande l'attribution d'une mise en forme différente si l'élément est différent.
3. **La rétroaction[51] immédiate :** assurer que les actions de l'utilisateur ne demeurent pas sans réponse. Par exemple, tous les hyperliens doivent être fonctionnels.
4. **La lisibilité (à l'écran) :** adapter l'information pour qu'elle soit visuellement lisible et identifiable. Elle doit être présentée avec un format sobre et adéquat (couleur, design, taille de police, interlignage, etc.) et être divisée de manière appropriée pour faciliter la lecture, ce qui implique de courts paragraphes, des listes à puces et le positionnement des hyperliens à l'extérieur des paragraphes. En effet, il semble que lorsqu'un paragraphe est parsemé d'hyperliens, la lecture devient fragmentaire[52], ce qui contrevient à la lisibilité.

2.3.2. DEUXIÈME CRITÈRE : LA CHARGE DE TRAVAIL

Dans ce contexte, la charge de travail réfère à l'ensemble des tâches que l'utilisateur doit effectuer pour combler ses attentes. Afin de réduire au maximum cette tâche de travail, deux sous-critères doivent être respectés :

1. **La brièveté :** privilégier des libellés d'hyperlien concis dans le menu pour éviter de l'« alourdir » inutilement, et assurer la faible profondeur de la navigation (nombre de clics réduits pour obtenir la page recherchée)[53].

---

[50]CLERC, I. et É. KAVANAGH – GOUVERNEMENT DU QUÉBEC. *De la lettre à la page Web : Savoir comment communiquer avec le grand public*,p. 294 – 330.

[51]Pour décrire ce sous-critère, Scapin et Bastien emploient le terme « *feedback* ». Dans le cadre de cette recherche, le mot « rétroaction » a été préféré à l'anglicisme « *feedback* ».

[52]CLERC, I. et É. KAVANAGH – GOUVERNEMENT DU QUÉBEC. *De la lettre à la page Web : Savoir comment communiquer avec le grand public*, p. 325.

[53] L'utilisateur a ainsi accès plus rapidement à l'information qu'il cherche.

2. **La densité informationnelle :** choisir uniquement les contenus pertinents pour le public cible et donner d'abord accès à des versions synthétisées des contenus plus longs.

2.3.3. TROISIÈME CRITÈRE : LE CONTRÔLE « EXPLICITE »

Lorsqu'un utilisateur interagit avec un site Web, ses actions doivent provoquer une réponse univoque (ou « explicite »). Les résultats obtenus ne doivent pas être inattendus ou incohérents; ils doivent correspondre aux requêtes de l'utilisateur, ce qui lui permettra de prendre le contrôle de sa navigation. Ce critère comporte deux sous-critères :

1. **Les actions « explicites » :** assurer que chacune des actions de l'utilisateur produise le résultat souhaité (par exemple, un clic sur le bouton « Envoyer » dans un formulaire doit proprement envoyer ce formulaire) et surtout, qu'aucune action ne se produise sans avoir été sollicitée (par exemple, un avis complémentaire, donc non obligatoire, ne doit pas s'afficher sans qu'une requête n'ait été formulée).
2. **Le contrôle utilisateur :** permettre à l'utilisateur de contrôler sa navigation sans difficulté, avec une suite d'actions « explicites ». Par exemple, s'il a l'impression de ne pas être sur la bonne page, il doit pouvoir cliquer sur « Accueil » dans le menu pour revenir au point de départ du site.

2.3.4. QUATRIÈME CRITÈRE : L'ADAPTABILITÉ

L'adaptabilité fait référence à la souplesse de l'interface et de la structure d'un site Web. Elle comprend deux sous-critères :

1. **La flexibilité :** donner à l'utilisateur la possibilité de « personnaliser » l'interface du site qu'il consulte. Il y a bien sûr les nouvelles technologies Web dynamiques (dont les applications Web) qui offrent un haut niveau de personnalisation[54]. Mais les sites à programmation « simplifiée » peuvent également être personnalisés (à plus petite échelle) grâce, entre autres, à quelques manipulations des paramètres du navigateur. Par exemple, si un utilisateur a de la difficulté à visualiser le contenu du site, il doit

[54] On n'a qu'à penser aux plateformes de courriel en ligne, comme Hotmail (http://www.hotmail.com) et Gmail (http://www.gmail.com), qui permettent les changements de couleur, la création de dossiers personnalisés à des fins de classification, et bien plus encore.

pouvoir agrandir la taille de la police et des images[55]. Évidemment, pour qu'une telle personnalisation soit possible, le site doit avoir été adéquatement conçu.

2. **La prise en compte de l'expérience utilisateur :** simplifier au maximum la structure d'un site pour faciliter la navigation, surtout lorsque le site en question est destiné à un public d'utilisateurs moyens. Il faut tout mettre en œuvre pour éviter que l'utilisateur se sente désorienté.

2.3.5. CINQUIÈME CRITÈRE : LA GESTION DES ERREURS

Les erreurs sont malheureusement inévitables lorsqu'on travaille avec l'informatique, raison pour laquelle elles doivent être proprement gérées. Pour y arriver, trois sous-critères doivent être pris en considération :

1. **La protection contre les erreurs :** concevoir le site Web avec l'intention de minimiser le risque d'erreurs, par exemple avec une programmation soignée.
2. **La qualité des messages d'erreurs :** utiliser des messages clairs et bien rédigés pour signaler les erreurs. Si un utilisateur est confronté à un message d'erreur bâclé ou imprécis, il peut ne pas comprendre son erreur, ce qui le met dans une position insatisfaisante.
3. **La correction des erreurs :** offrir aux utilisateurs la possibilité de signaler une erreur rencontrée aux responsables concernés.

2.3.6. SIXIÈME CRITÈRE : L'HOMOGÉNÉITÉ ET LA COHÉRENCE (CONSTANCE)

Toutes les pages d'un site correspondant à un même contexte doivent utiliser la même interface. Le non-respect de cette règle peut créer une désorientation chez les utilisateurs. Par exemple, si une page affiche soudainement un menu ou un en-tête différent, il y a alors une brèche dans l'homogénéité. En contrepartie, si le contexte d'affichage est différent (par exemple, si la page est destinée exclusivement à l'impression), l'interface doit l'être également.

2.3.7. SEPTIÈME CRITÈRE : LA SIGNIFIANCE DES CODES ET DES DÉNOMINATIONS (L'ADAPTATION ET LA VULGARISATION)

Dans un site Web, il ne suffit pas de transmettre le contenu, il faut le rendre compréhensible pour le public visé. Puisque le site du présent projet est majoritairement destiné à un public

[55]Dans le navigateur Mozilla Firefox, ce paramètre est accessible par le menu Affichage / Zoom.

d'utilisateurs moyens, avec une connaissance limitée de la sécurité Internet, l'adaptation et la vulgarisation s'avèrent essentielles, entre autres parce qu'il s'agit d'un contenu à haute teneur informatique susceptible de contenir du jargon technologique.

L'adaptation et la vulgarisation passent non seulement par le langage (« technologique », « formel », familier, etc.) et le style (voix active et forme interrogative[56]) employés, mais également par l'utilisation de phrases et de paragraphes courts (ce qui répond également au critère du guidage) et d'un vocabulaire accessible. Doivent également être exclus les termes issus d'un jargon technologique ou, s'ils sont inévitables, il doivent être expliqués à l'aide de définitions éclairées d'**exemples** ou de compléments graphiques pertinents, ou encore soumis à **des procédés de reformulation**[57] dont :

- la **comparaison**, qui met en relation un comparant et un comparé pour évaluer leur ressemblance ou leur différence. Exemple : *L'espiogiciel est comme un petit espion, tout de noir vêtu, épiant chacun de vos gestes dans l'objectif ultime de placarder chaque mur de votre maison avec des publicités en tous genres.*
- la **métaphore**, qui implique l'emploi d'un terme concret pour expliquer une notion abstraite. Exemple : *Le* rootkit, *c'est le magicien des menaces Internet. [...] Il arrive en effet à faire « disparaître » toute trace de sa présence.*
- L'**analogie**, qui désigne le rapport entre des éléments qui ont des similitudes. Exemple : *Certains [chevaux de Troie] vont se concentrer sur l'ouverture d'une porte dérobée pour permettre à un (ou plusieurs) pirate de s'introduire dans l'ordinateur infecté. En guise d'analogie, c'est un peu comme si un criminel s'infiltrait dans votre maison et en profitait pour inviter d'autres malfrats, tout ça à votre insu.*

2.3.8. HUITIÈME CRITÈRE : LA COMPATIBILITÉ (L'ACCESSIBILITÉ)

Dans le contexte d'un site Web, ce critère de compatibilité s'applique à l'interface, qui doit s'adapter à l'environnement technologique de chaque visiteur. Elle doit être conçue avec des technologies accessibles, soit celles qui permettent un affichage adéquat du site sur n'importe

[56]MALAVOY, Sophie. *Guide pratique de vulgarisation scientifique*, Montréal, Acfas, 1999, p. 25.
[57]JACOBI, Daniel. *La communication scientifique : discours, figures et modèles*, Coll. « Communication, Médias et Sociétés », Grenoble, Presses Universitaires de Grenoble, 1999, p. 83-86.

quel ordinateur, peu importe le type (ordinateur PC ou Mac*) et les logiciels installés (système d'exploitation et navigateur).

2.4. LA CRÉATION DE L'OUTIL

Ces critères méthodologiques ont guidé la création du site Web destiné aux internautes moyens, un outil en ligne utile et utilisable pouvant être consulté à l'adresse http://pages.usherbrooke.ca/securite_internet101/[58]. De plus, pour faciliter la tâche des correcteurs, un exemplaire navigable hors ligne de ce site est disponible sur le support cédérom joint au présent document imprimé. Pour entamer la consultation, il suffit de double-cliquer sur le fichier « index.html ».

[58]L'élaboration de cet outil s'est échelonnée sur deux années complètes.

3. RETOUR SUR LA PRODUCTION

La création du site Web sur la sécurité Internet a été divisée en trois étapes : la préproduction, l'élaboration des contenus, et la conception et mise en ligne du site en soi. Une postproduction a été anticipée, mais elle ne sera pas abordée en détail, puisqu'elle déborde du cadre du projet. Chaque étape a été complétée en tenant compte à la fois de l'état de la question, de l'objectif de recherche et des critères identifiés dans la méthodologie. Il est important de préciser que certains aspects du projet initial (présentés dans le projet de recherche) ont dû subir des modifications (élaborés au point 3.3.3), dûment documentées, afin, entre autres, d'assurer l'atteinte de l'objectif et le respect des critères méthodologiques.

3.1. LA PRÉPRODUCTION

Avant d'entamer les importantes étapes de l'élaboration des contenus et de la conception du site, il était nécessaire d'identifier les contenus à traiter, de dresser une structure permettant de les classer et de créer un titre représentatif.

3.1.1. L'IDENTIFICATION DES CONTENUS ET L'ÉTABLISSEMENT DE LA STRUCTURE DU SITE

En premier lieu, afin que le site soit en mesure de fournir des explications claires et abordables sur les menaces les plus courantes sur Internet, il convenait d'identifier ces principales menaces. Chacune d'elles a été choisie en fonction de sa **fréquence** (par exemple, une menace très courante) et de la **portée de ses conséquences** (par exemple, une nouvelle menace qui, avec une seule attaque, fait beaucoup de dommages et atteint un grand nombre de victimes) dans le contexte Internet actuel, où les risques sont liés aux logiciels et aux comportements de leurs utilisateurs. Celles qui étaient désuètes ou trop rares ont été exclues. Il est important de mentionner que des spécialistes de la sécurité informatique de l'ISIQ ont été consultés afin de valider la liste finale des menaces retenues.

Les menaces correspondant aux conditions précédemment énumérées ont été identifiées (voir le point 1.1.3), puis classées selon leur nature dans les catégories « Logiciels malveillants » et « Autres types de fraudes ou tromperies »[59]. Différentes catégorisations ont été testées, mais cette dernière a été retenue pour sa simplicité et son univocité.

[59]Aperçu de la classification et des menaces retenues (visibles dans le menu de gauche) : http://pages.usherbrooke.ca/securite_internet101/menaces.html

En second lieu, au fil du développement du site, de nouveaux besoins sont apparus. Au-delà de la description et du classement des menaces, des moyens de protection et des solutions de cure, l'ajout de définitions (essentielles à l'adaptation et à la vulgarisation), d'une forme d'aide au diagnostic et de contenus abordant des sujets d'actualité (par exemple, Facebook), ou connexes à la sécurité Internet (par exemple, le choix d'un bon mot de passe), s'est imposé. Cette observation a mené ultimement à la création des rubriques « Glossaire », « Aide au diagnostic » et « Faits divers ».

Une fois les contenus identifiés, une structure a pu être établie afin de discerner les limites de l'élaboration des contenus. La structure finale du site est résumée à l'annexe 3 du présent document.

3.1.2. LA CRÉATION DU TITRE DU SITE

Le titre devait être représentatif du risque actuel (issu tant des technologies que des comportements des internautes), tout en reflétant la nature des contenus du site (menaces, aide au diagnostic, etc.), les différents aspects abordés (prévention, diagnostic et cure) et le niveau de connaissance du sujet par le public ciblé. Plusieurs titres ont été envisagés, dont *Petit guide d'autodéfense contre les menaces sur Internet*, mais *Sécurité Internet 101 : Technologie et comportement* a été retenu, car il répondait mieux aux quatre critères ci-haut mentionnés. De plus, les termes simples et explicites du titre conféraient au site une « valeur ajoutée » dans les moteurs de recherche en facilitant son repérage.

3.2. L'ÉLABORATION DES CONTENUS

Une fois les contenus identifiés et leur structure de présentation validée, il s'agissait de les élaborer. Des recherches approfondies ont été effectuées méthodiquement pour documenter les menaces et les rubriques complémentaires. S'ensuivait la rédaction proprement dite, qui devait respecter certains critères d'adaptation et de vulgarisation, pour offrir un maximum d'utilisabilité, et tenir compte de l'évolution du sujet (expliquée au point 3.2.2.2).

3.2.1. LA RECHERCHE D'INFORMATION ET LE TRI

Afin d'élaborer les contenus du site, une grande recherche d'information a été entamée. La documentation recueillie a par la suite été triée.

1. **Le repérage :** pour repérer l'information pertinente, différentes sources, sur supports virtuels ou papiers, tant francophones qu'anglophones, ont été consultées :
   - des livres spécialisés (par exemple, *Hacking interdit*[60], de Alexandre Gomez Urbina);
   - des sites Web généralistes (par exemple, Wikipedia[61]);
   - des sites Web spécialisés (par exemple, Assiste[62]);
   - des périodiques imprimés spécialisés (par exemple, *Micro hebdo*[63]);
   - des périodiques en ligne spécialisés (par exemple, *DirectionInformatique.com*[64]);
   - des forums spécialisés (par exemple, Commentçamarche.net[65]);
   - des blogues spécialisés (par exemple, le blogue de Nelson Dumais, spécialiste québécois de l'informatique[66]).
2. **L'appropriation de l'information complexe :** certains sujets abordés étaient complexes. Des recherches et des lectures supplémentaires ont été nécessaires pour bien les comprendre et, ainsi, être en mesure de cibler et retenir l'information pertinente.
3. **Un premier tri :** parmi toutes les sources consultées, force était de constater qu'il y avait une quantité trop imposante de sites Web spécialisés traitant de sécurité Internet. La crédibilité de certains sites pouvait parfois être remise en question. Les sites repérés ont donc été soumis à un juste contrôle de la qualité[67] pour éliminer ceux pouvant être jugés non crédibles.
4. **Un second tri :** l'amas d'information issu du premier tri, quoique réduit, demeurait important et révélait l'abondance de matière sur le sujet de la sécurité Internet. Un

---

[60]GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition,* Coll. « microapp », Paris, Micro Application, 2007, 1247 p.
[61]WIKIPEDIA. *Wikipedia, the free encyclopedia*, 2010, http://en.wikipedia.org/wiki/Main_Page.
[62]PINARD, Pierre. *Assiste.com – Sécurité informatique et protection de la Vie privée sur l'Internet*, 2008, http://assiste.com.free.fr/index.html.
[63]*Micro hebdo*, n° 608 (semaine du 10 décembre au 16 décembre 2009)- , Paris, Groupe 01.
[64]DIRECTION INFORMATIQUE. *Direction informatique | technologies de l'information, TI, communications, stratégies*, 2010, http://www.directioninformatique.com/.
[65]COMMENTCAMARCHE.NET. *Forum d'assistance informatique*, 2010, http://www.commentcamarche.net/forum/.
[66]DUMAIS, Nelson. *La chronique de Nelson*, 2010, http://blogues.cyberpresse.ca/technaute/dumais/.
[67]Pour vérifier la crédibilité d'un site Web, l'étudiante a consulté des forums ou des blogues spécialisés, ou a effectué une vérification auprès d'un spécialiste de la sécurité informatique de l'ISIQ.

second tri, basé cette fois-ci sur la pertinence des sources (tant sur le Web que sur un support papier), a été effectué.

5. **Un troisième tri :** un dernier tri s'imposait pour ne conserver que la documentation la plus utile et surtout, la plus « solide », c'est-à-dire celle qui peut difficilement être contredite. Toute ressource présentant des contradictions ou des erreurs, ou avançant des conclusions hasardeuses ou marginales, a été rejetée.

Cette recherche méthodique a permis de recueillir l'information nécessaire à l'élaboration du glossaire et des contenus sur les menaces. Toutefois, pour développer les contenus de l'aide au diagnostic, la recherche a dû être étendue au-delà des limites des médias et des spécialistes de la sécurité, vers les internautes eux-mêmes. De l'information a été recueillie de manière informelle auprès d'un petit échantillon ad hoc d'individus[68] aux profils semblables à celui du public cible, peu connaissants en matière de sécurité Internet, afin d'en savoir plus sur les principales difficultés qu'ils vivaient lorsqu'ils étaient connectés. Par exemple, ils se retrouvaient souvent sans moyens devant un bogue logiciel, un avis ou un texte incompréhensible, ou un simple questionnement qu'ils n'osaient pas formuler à un spécialiste. Une fois leurs problématiques recueillies, des solutions ont été pensées et documentées, ce qui a permis la création d'une aide au diagnostic davantage adaptée à la réalité des internautes.

3.2.2. LA RÉDACTION DES CONTENUS DU SITE

En raison du public cible, les contenus devaient être adaptés et vulgarisés, donc clairs et compréhensibles. Il s'agit là du septième critère ergonomique de Scapin et Bastien, la signifiance des codes et dénominations[69].

De plus, il est important de préciser que, comme la sécurité Internet est un sujet en constante évolution, certains contenus sont devenus désuets en cours de rédaction et ont dû être mis à jour, parfois à plusieurs reprises, tel que détaillé au point 3.2.2.2.

[68]Cinq personnes connues par l'étudiante (amis et famille) ont fait part, au cours de discussions informelles, de problématiques personnelles vécues lors de l'utilisation d'Internet.

[69]Les réalisations correspondant au septième critère de Scapin et Bastien sont ici abordées. Les applications quant aux sept autres critères sont élaborées au point 3.3.1.

3.2.2.1. LA SIGNIFIANCE DES CODES ET DES DÉNOMINATIONS (L'ADAPTATION ET LA VULGARISATION)

L'étudiante s'est efforcée de rédiger les contenus dans un langage clair (et plus « technologique » si nécessaire) à la voix active (interpellant parfois directement l'internaute) et sous une forme interrogative lorsque requis. De plus, l'emploi des termes issus d'un jargon technologique a été limité; ils n'ont été utilisés que lorsque c'était inévitable. Dans ces cas précis, des compléments graphiques, des définitions ou des exemples se sont ajoutés aux termes concernés, ou ils étaient soumis à des procédés de reformulation. La comparaison et l'analogie ont d'ailleurs été les procédés les plus fréquemment mis en œuvre.

Toujours dans le domaine de l'adaptation et de la vulgarisation, la synthèse, étape liée au critère de la charge de travail, a été essentielle à plusieurs reprises pour faire ressortir les éléments cruciaux, tout en permettant à l'utilisateur une économie d'efforts dans sa recherche de contenu. Par exemple, les rubriques sur les menaces, très chargées, ont toutes été précédées d'une version sommaire proprement synthétisée.

Les textes, en plus d'être divisés en courts paragraphes (ce qui répond aussi au critère du guidage), ont été « parsemés » d'encadrés, sous différentes bannières colorées[70], pour stimuler la lecture. Par exemple, un encadré « Question » a été créé pour mettre en évidence une question qu'un internaute pourrait être porté à se poser en lisant le contenu. La réponse à cette question est également présentée et constitue une information complémentaire qui aide l'internaute à comprendre.

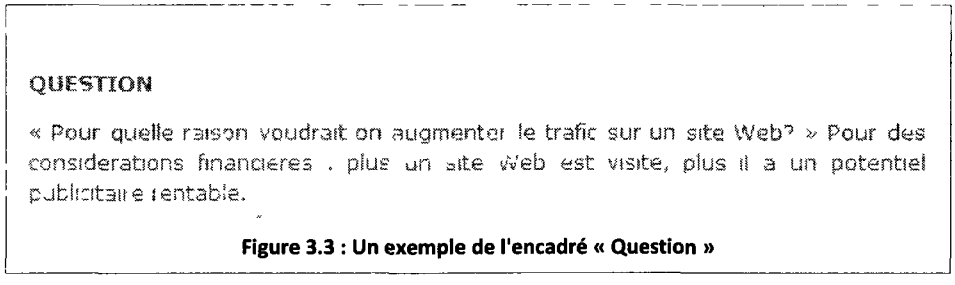


Figure 3.3 : Un exemple de l'encadré « Question »

L'interface du site en soi a aussi contribué à l'adaptation et à la vulgarisation (en plus de répondre au sous-critère de la lisibilité) de par sa structure hiérarchique, la simplicité des menus et la sobriété voulue du graphisme. Finalement, il ne faut pas négliger l'apport du média dans son

[70]Les étiquettes de bannières sont les suivantes : « Attention », « Culture générale », « Important », « Question » et « Rappel »

ensemble. En effet, le site Web a permis d'adapter des contenus linéaires en contenus dynamiques et interactifs, ce qui facilite la tâche de compréhension.

Exemple de dynamisme :

Les infobulles* de définition : pour plusieurs mots issus du jargon[71], une définition, présentée dans une infobulle, a été ajoutée. L'utilisateur peut ainsi la consulter rapidement, sans avoir à visiter une autre page.

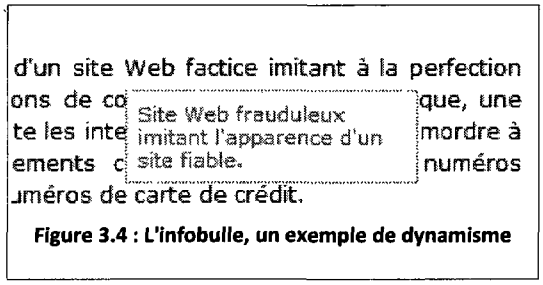


Figure 3.4 : L'infobulle, un exemple de dynamisme

Exemples d'interaction :

1. **La liste personnalisée de bonnes attitudes et habitudes** (voir Figure 3.5 à la page suivante) : cette fonctionnalité a été mise sur pied pour permettre aux utilisateurs de se créer un aide-mémoire personnalisé sur la sécurité Internet. Ils sont d'abord invités à cocher certains éléments « globaux » dans une liste de cases à cocher. Une sélection provoque le déploiement d'une seconde liste « détaillée », volontairement masquée pour limiter la densité informationnelle de la page (selon le critère ergonomique de la charge de travail), et ils doivent ensuite poursuivre leurs sélections. Finalement, ils peuvent imprimer l'ensemble des éléments sélectionnés.

[71]Fait à noter, dans une page entière, seule la première occurrence du mot comportait une infobulle de définition.

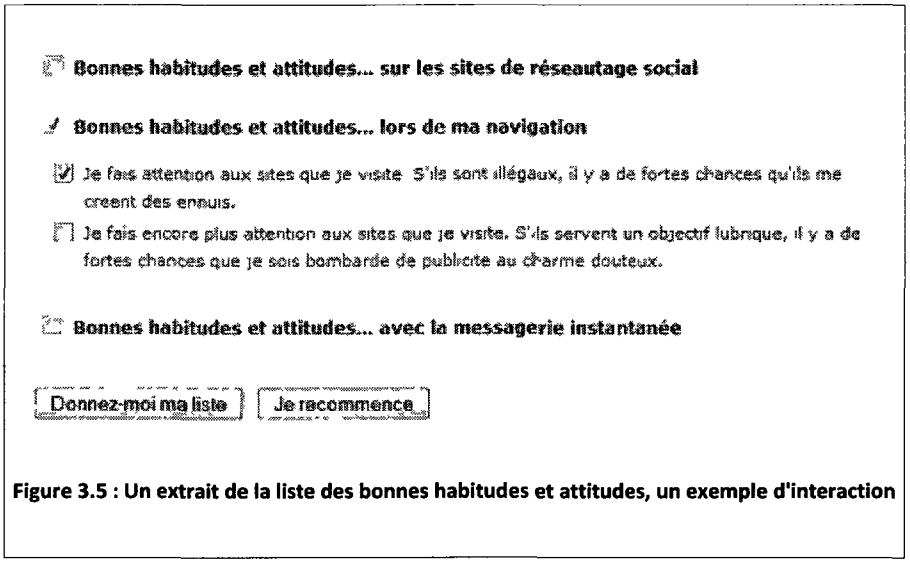


Figure 3.5 : Un extrait de la liste des bonnes habitudes et attitudes, un exemple d'interaction

2. **Les questions et réponses :** cette section a été programmée pour n'afficher que les questions, les réponses n'apparaissant qu'au gré des clics de l'internaute.

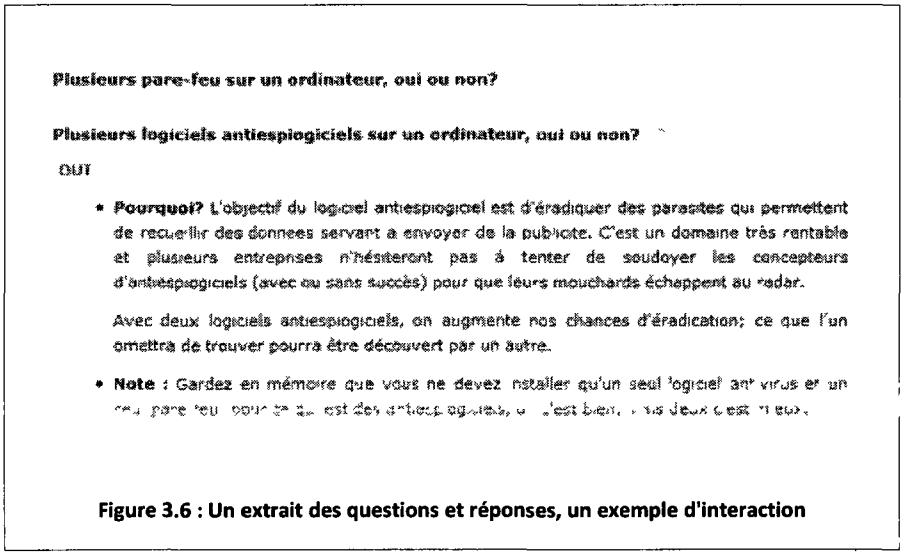


Figure 3.6 : Un extrait des questions et réponses, un exemple d'interaction

3.2.2.2. L'ÉVOLUTION DU SUJET ET LA CRÉDIBILITÉ

Tout sujet touchant à l'informatique et au Web évolue rapidement. Durant l'élaboration des contenus, et même après, de nouvelles menaces ont fait surface, de nouvelles données ont altéré, voire fait chavirer, certaines affirmations, des problèmes sont apparus et des solutions se sont avérées plus pertinentes que celles déjà présentées. Par exemple, l'explosion soudaine vers la fin

de 2008 d'une menace alors peu répandue, le faux logiciel de sécurité, a nécessité la création de nouveaux contenus, avec son lot de recherche et d'écriture.

Dans chacun des cas, des modifications et (ou) des ajouts, parfois importants et parfois mineurs, ont dû être apportés aux contenus concernés, sans quoi leur pertinence et leur utilité pouvaient être remises en question. À cet effet, la datation des contenus s'est avérée très importante. Grâce à la date affichée, l'internaute est en mesure de juger rapidement de la récence du texte qu'il consulte et donc, de son utilité.

De plus, dans un monde où le nombre de « spécialistes » autoproclamés de la sécurité Internet ne cesse d'augmenter, tout élément pouvant renforcer la crédibilité du site a dû être mis de l'avant. Par exemple, le contexte d'élaboration du site Web a été affiché sur chaque page[72]. Il est possible d'avancer que la mention « Université de Sherbrooke » contribue à rassurer l'internaute dans son choix de ressource.

3.3. LA CONCEPTION DU SITE

Pour que le site soit ergonomique, il devait, en plus de proposer des contenus utiles et utilisables (dans le sens d'« abordables »), offrir une interface utilisable, c'est-à-dire facilement manipulable. Ces deux volets de l'ergonomie Web (utilité et utilisabilité) sont indissociables, car les lacunes en utilisabilité affectent directement l'utilité.

3.3.1. LA CRÉATION DE L'INTERFACE GRAPHIQUE

L'interface graphique est la concrétisation visuelle de la structure d'un site Web et elle rassemble toutes les composantes nécessaires à sa manipulation. Pour être utilisable, elle devait donc respecter les critères ergonomiques de Scapin et Bastien concernés, soit le guidage, la charge de travail, le contrôle « explicite », l'adaptabilité, la gestion des erreurs, l'homogénéité et de la cohérence, et la compatibilité (ou accessibilité)[73]. Voici ce qui a été mis en place pour chacun de ces critères.

---

[72]Le message suivant figure au bas de chaque page du site : « Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet, Maîtrise en études françaises, cheminement communication et langage, Université de Sherbrooke, 2010 ».

[73]Seuls sept critères ergonomiques de Scapin et Bastien sont ici énumérés (les critères un à six, et le huitième). Le septième critère, la signifiance des codes et des dénominations (l'adaptation et la vulgarisation), est abordé en détail au point 3.2.2.1.

3.3.1.1. LE GUIDAGE

- L'incitation
    - Des titres clairs et représentatifs ont été utilisés sur toutes les pages. En plus de se trouver dans la barre de titre*, ces repères de position, localisés au haut de la page, sont facilement repérables dès la consultation[74] de cette page.
    - Un fil d'Ariane a été ajouté sur chacune des pages et il agit à titre de repère de position.
    - Un plan du site, une sorte de « table des matières » globale, a été créé et il est accessible par un hyperlien sur chaque page. Il agit comme une aide à la navigation.
    - Les hyperliens dans le contenu (excluant ceux du menu) ont été programmés pour être immédiatement reconnaissables : ils sont tous soulignés, capitalisant ainsi sur une connaissance acquise chez les utilisateurs. Les hyperliens des infobulles sont toutefois différents, car ils devaient se « fondre » au texte pour éviter de fragmenter la lecture. Mais un internaute attentif saura les reconnaître par leur soulignement discret.
    - Les hyperliens ont tous été « contextualisés »[75], ce qui signifie qu'ils sont balisés d'un texte identifiant clairement le contexte de la page obtenue à la suite du clic. Par exemple, sur la page décrivant le cheval de Troie, l'utilisateur sait que s'il clique sur « Qu'est-ce que c'est? », il sera dirigé vers le contenu expliquant la nature de la menace. De plus, deux couleurs d'hyperliens ont été utilisées : l'une pour les hyperliens internes (menant vers des pages à l'intérieur du site) et l'autre pour les hyperliens externes (menant vers des pages à l'extérieur du site). Cette façon de faire permet aux internautes de comprendre d'un seul coup d'œil le contexte de l'hyperlien. Cette norme est d'ailleurs expliquée dans les conditions d'utilisation (http://pages.usherbrooke.ca/securite_internet101/conditions.html#hyperliens).

[74]CLERC, I. et É. KAVANAGH – GOUVERNEMENT DU QUÉBEC. *De la lettre à la page Web : Savoir comment communiquer avec le grand public*, p. 310.
[75]*Idem*, p. 321.

- Le groupement et la distinction
    - Pour éviter toute confusion, le menu principal (au haut de l'écran, à l'horizontale) regroupe les éléments à la base de la navigation et chacun d'eux est univoque. Un sous-menu pertinent (à gauche de l'écran, à la verticale) est associé à chaque élément du menu principal, une façon qui permet à l'internaute de pouvoir « évaluer » rapidement le « micromonde » de contenu qui s'offre à lui à la suite d'une sélection dans le menu principal.

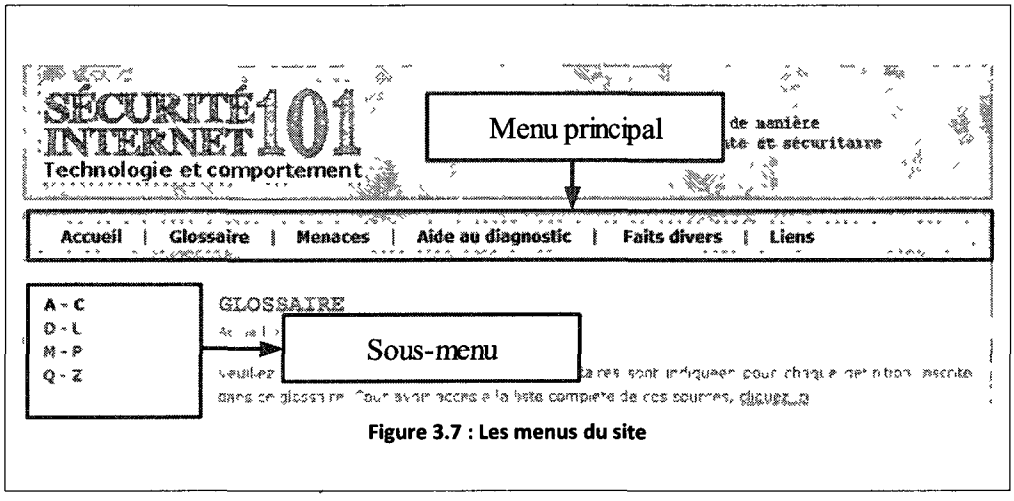


Figure 3.7 : Les menus du site

    - Chaque menu est positionné dans un espace précis; il y a donc une zone pour le menu principal et une autre pour le sous-menu (voir Figure 3.7). De cette manière, aucun sous-menu ne se « déroule » sous le menu principal, il apparaît plutôt systématiquement dans son espace dédié, facilement repérable par l'internaute. Cette simplicité et cette systématicité répondent à la fois au critère de l'adaptation et de la vulgarisation, et à celui du guidage.
- La rétroaction immédiate
    - Le site a été programmé pour que chaque action commise par l'utilisateur provoque une réaction. Il y a, entre autres, l'activation d'un formulaire par un clic sur le bouton approprié (par exemple, le formulaire « Contact » comprend un bouton « Envoyer » qui permet à l'utilisateur de le soumettre) et le survol de

certains mots qui déclenche l'affichage d'une infobulle proposant une définition (expliquée au point 3.2.2.1).

- La lisibilité (à l'écran)
    - Le choix s'est arrêté sur une interface dépouillée, alliant des couleurs qu'on peut qualifier de « calmes » et « sobres » (le bleu et le blanc), sur une structure simple et sur une mise en page aérée. Une telle interface permet aux utilisateurs, toutes compétences informatiques confondues, de décoder rapidement l'architecture du site[76] sans être dérangés par des éléments graphiques superflus. Elle contribue aussi à l'adaptation et à la vulgarisation et répond au critère du guidage.
    - L'interface a été optimisée pour favoriser la lecture à l'écran (taille de police de 10 ou 12 points, interlignage raisonnable et couleurs de texte contrastées).
    - L'emploi de courts paragraphes, la division des longs textes en sections titrées et sous-titrées, et l'utilisation des listes à puces, ont été privilégiés, ce qui contribue non seulement à l'adaptation et à la vulgarisation, mais respecte également le critère du guidage.
    - Dans la mesure du possible, et sauf pour les infobulles, les hyperliens ont été placés à l'extérieur des paragraphes, une pratique souhaitable, car elle « allège » le texte et facilite sa lisibilité; les hyperliens se situent plutôt dans des listes à puces situées sous les paragraphes concernés.

3.3.1.2. LA CHARGE DE TRAVAIL

- La brièveté
    - Les libellés des hyperliens qui composent le menu principal et le sous-menu sont concis et ne sont pas « alourdis » par des mots non significatifs (comme des articles ou des adjectifs superflus), ce qui facilite la tâche de « décodage » des utilisateurs.
    - La navigation du site n'est pas très « profonde ». Sa structure a été pensée pour que l'utilisateur ait un minimum de clics à effectuer pour obtenir la page souhaitée. Par exemple, à partir de la page d'accueil, trois clics (ce qui constitue un idéal) sont

[76]CLERC, I. et É. KAVANAGH – GOUVERNEMENT DU QUÉBEC. *De la lettre à la page Web : Savoir comment communiquer avec le grand public*, p. 287.

nécessaires pour savoir comment prévenir et guérir une infection par un ver informatique.

- La densité informationnelle
    - Il était important de donner d'abord accès à une version sommaire des contenus lourds. Ainsi, chaque menace décrite (des contenus riches et détaillés) est précédée d'une version résumée présentant les deux principaux points d'intérêt, « Qu'est-ce que c'est? » et « Comment prévenir et guérir? ». Puis, en cliquant sur « Plus », les utilisateurs peuvent obtenir la version complète. La tâche de l'utilisateur s'en trouve considérablement réduite, puisqu'il n'a pas à « absorber » une masse de contenus qui s'avéreraient non pertinents compte tenu de son problème actuel. Une telle mesure a un impact important sur l'utilisabilité du site en entier.
    - Des définitions des termes technologiques, ou issus d'un jargon, ont été programmées pour apparaître dans une infobulle par un simple survol mot avec le curseur, ce qui évite à l'utilisateur d'avoir à consulter le glossaire chaque fois qu'il en ressent le besoin. Cette particularité contribue autant à l'adaptation et à la vulgarisation qu'à la réduction de la charge de travail, en plus d'apporter une bonne contribution à l'utilisabilité du site dans son ensemble.
    - La section « Questions et réponses », détaillée au point 3.2.2.1, a été conçue de sorte que seules les questions apparaissent lors de l'activation de la page. Les réponses ne sont affichées qu'à la demande de l'utilisateur, ce qui contribue autant à l'adaptation et à la vulgarisation qu'à la réduction de la densité informationnelle. La « Liste des bonnes habitudes et attitudes », présentée au point 3.2.2.1, respecte également de principe.

3.3.1.3. LE CONTRÔLE « EXPLICITE »

- Les actions « explicites »
    - Certaines fonctionnalités du site, à savoir la « Liste des bonnes habitudes et attitudes » et le formulaire « Contact », peuvent ne pas être suffisamment « explicites » sans indications claires. Leur conception a donc requis certains perfectionnements pour en faciliter la prise de contrôle.

- La « Liste des bonnes habitudes et attitudes » est divisée en catégories univoques et mutuellement exclusives, la validation du formulaire est clairement identifiée (« Donnez-moi ma liste ») et quelques instructions sont offertes dans le sous-menu. Lorsque l'extrant (une liste à imprimer) est obtenu, il est facilement manipulable. L'utilisateur peut aisément revenir à son point de départ sans voir la liste disparaître, puisqu'elle s'affiche dans une fenêtre distincte.
- Le formulaire « Contact » est succinct, sa validation est clairement identifiée (« Envoyer ») et il présente à l'utilisateur un message d'erreur adapté lorsque requis.

- Aucune opération n'a été programmée pour s'exécuter automatiquement, sans commande de l'utilisateur. Par exemple, si ce dernier souhaite obtenir des instructions sur l'utilisation de la Liste des bonnes habitudes et attitudes, il doit glisser son curseur sur le lien à cet effet. Les instructions sont complémentaires (et non obligatoires à la manipulation de la fonctionnalité), donc elles ne s'affichent pas automatiquement. De plus, s'il désire imprimer l'extrant de la Liste des bonnes habitudes et attitudes, il doit cliquer sur le lien à cet effet; cette action ne s'exécutera pas automatiquement.

- Le contrôle utilisateur
  - En tout temps, l'utilisateur peut revenir au point de départ du site (la page d'accueil) en cliquant sur le menu « Accueil » ou sur le logo présent dans l'en-tête graphique.
  - Il est pertinent d'ajouter que des mesures ont été mises en place pour renforcer le sentiment de sécurité des utilisateurs, ce qui les met en bonne position pour prendre pleinement contrôle de leur navigation.
    - Aucun renseignement inscrit dans les formulaires n'est conservé, ce qui est clairement indiqué sur chaque page concernée (avec un avis rouge dans le sous-menu) et dans les conditions d'utilisation (http://pages.usherbrooke.ca/securite_internet101/conditions.html#confidentialite).

- Dans le formulaire « Contact », un champ de vérification (une simple question – http://pages.usherbrooke.ca/securite_internet101/contact.html) a été ajouté pour vérifier que l'utilisateur qui soumet le formulaire n'est par un « robot spammeur[77] ».

3.3.1.4. L'ADAPTABILITÉ

- La flexibilité
  - L'interface a été programmée pour que les utilisateurs puissent agrandir la taille de la police et celle des images à leur guise, en manipulant un paramètre du navigateur[78].
  - L'interface a été optimisée pour l'impression, de sorte que chaque page, en plus de s'afficher dans un format approprié pour la consultation à l'écran, est imprimable dans un format adapté au support papier (grâce à des paramètres de la feuille de style relatifs à l'impression). Cette caractéristique sécurise l'internaute, qui a la possibilité d'obtenir une version imprimable facile à consulter en cas de besoin, par exemple en cas de perte de connectivité.
  - Le format de l'interface s'adapte aux résolutions d'écran les plus populaires[79], 1024 x 768 et 1280 x 800, de même qu'à la résolution 800 x 600.
- La prise en compte de l'expérience utilisateur
  - Tel qu'indiqué au point 2.2.1, le site est destiné en priorité à un public d'utilisateurs moyens, donc son interface et ses contenus ont été adaptés pour cet auditoire.

3.3.1.5. LA GESTION DES ERREURS

- La protection contre les erreurs
  - Un soin particulier a été apporté à la programmation pour limiter les erreurs. Seules les technologies « standard » ont été employées (HTML*, CSS*, etc.), ce qui évite à l'utilisateur d'avoir à manipuler un plugiciel, manipulation pouvant être interprétée, parfois à tort, comme une erreur.

---

[77]Traduction libre de *spambot*. Il s'agit d'un petit dispositif qui peut inscrire dans un formulaire un message publicitaire pour ensuite le soumettre à plusieurs reprises afin de « polluer » la boîte courriel du destinataire.
[78]Dans le navigateur Mozilla Firefox, ce paramètre est accessible par le menu Affichage / Zoom.
[79]NET MARKET SHARE. *Market share for browsers, operating systems and search engines, Screen resolutions*, juillet 2010, http://marketshare.hitslink.com/report.aspx?qprid=17.

- La qualité des messages d'erreur
    - Le formulaire « Contact » a été conçu pour que des messages adaptés s'affichent si l'utilisateur n'a pas inscrit un renseignement demandé (par exemple, s'il a oublié d'indiquer l'objet de son message) ou s'il a fourni de l'information erronée (par exemple, s'il a fait une erreur dans son adresse courriel). Cette fonctionnalité dynamique permet de répondre aux critères à la fois du contrôle « explicite » et de la gestion des erreurs.
- La correction des erreurs
    - Le formulaire « Contact » a été optimisé pour offrir la possibilité de signaler une erreur ou un bogue si une telle découverte survient.

3.3.1.6. L'HOMOGÉNÉITÉ ET LA COHÉRENCE

- L'en-tête, qui comprend le logo cliquable (vers la page d'accueil) et la composante graphique (une image composée d'un arrière-plan esthétique et de la phrase « Utiliser Internet de manière intelligente et sécuritaire »), a été ajouté sur toutes les pages du site, ce qui assure l'homogénéité et contribue à renforcer le sentiment de sécurité de l'internaute, puisqu'il sait qu'il se trouve toujours dans le même site. Le menu, quant à lui, est présent sur toutes les pages, à l'exception de l'extrant de la « Liste des bonnes habitudes et attitudes », destiné exclusivement à l'impression.
- La même mise en page (format, position de l'en-tête, structure du contenu) a été utilisée pour toutes les pages du site.

3.3.1.7. LA COMPATIBILITÉ (L'ACCESSIBILITÉ)

- Le HTML, qui est le langage de base pour la conception Web, a été choisi pour la partie documentaire et a été agrémenté de feuilles de style (CSS) pour gérer l'apparence du site. Pour conférer du dynamisme à quelques sections, le JavaScript* et le langage PHP*, tous deux accessibles, ont été utilisés. Des vérifications de base donnent certaines garanties quant à leur sécurité.
- Aucun contenu ne nécessitant l'activation d'un plugiciel n'a été ajouté au site.

3.3.2. LES CHANGEMENTS APPORTÉS POUR ASSURER L'UTILITÉ ET L'UTILISABILITÉ

En cours de conception, des changements ont dû être apportés au projet initial afin d'éviter toute lacune d'utilité et d'utilisabilité de manière à obtenir un outil répondant à l'objectif du projet. Le menu principal a été modifié, le « guide de recherche » initialement prévu a été remplacé par une série de questions et réponse, et une « Liste de bonnes habitudes et attitudes », et un formulaire de contact a été ajouté.

3.3.2.1. LE MENU PRINCIPAL

Essentiel à la navigation, le menu contribue directement à l'utilité d'un site Web. Le menu anticipé avant la programmation comprenait les cinq éléments suivants : Accueil, Menaces, Diagnostic, Téléchargement et Liens.

Bien que pertinent, ce menu n'était pas suffisamment utile. Il y manquait d'abord un élément important, le glossaire. Un accès facile et rapide au glossaire est rassurant, en plus de faciliter l'apprentissage. Ensuite, l'étiquette « Diagnostic » pouvait porter à confusion, puisque cette section ne permet pas l'obtention d'un diagnostic « final et irréversible »; elle fournit plutôt de l'aide aux internautes pour les amener à faire leur propre diagnostic (d'où le choix de l'étiquette finale « Aide au diagnostic »). Un autre constat a également fait surface : aucun élément n'introduisait une section dédiée aux contenus d'actualité ou connexes à la sécurité Internet (abordés au point 3.1.1). Une section supplémentaire s'avérait alors pertinente pour offrir des rubriques complètes sur ces sujets d'intérêt. Finalement, l'élément « Téléchargement » a été changé pour « Liens », permettant ainsi d'y regrouper un plus grand nombre de ressources supplémentaires (sites et téléchargements)[80], offertes sous la forme d'hyperliens.

[80]Tous les logiciels proposés en téléchargement sont gratuits et sont proposés sous la forme d'hyperliens vers les sites des concepteurs concernés.

3.3.2.2. LE « GUIDE DE RECHERCHE »

À l'origine, un « guide de recherche » était prévu dans la section « Aide au diagnostic » justement pour aider l'internaute dans sa recherche de solution[81]. Son objectif était de le soutenir pas à pas dans les démarches du processus de recherche, qui devait être progressif et l'amener à s'approprier une procédure de diagnostic par élimination, une étape à la fois (en répondant à des questions par « oui » ou « non »). Cette façon de faire avait été pensée pour permettre à l'internaute non seulement de trouver une réponse (savoir de quelle menace il était affligé), mais également de comprendre comment il en était arrivé à cette solution. Ce « guide de recherche » était associé à un processus de résolution de problème et il pouvait également servir à des fins préventives, pour la simple recherche d'information[82].

Le développement de ce guide avait été divisé en deux étapes : il devait d'abord être pensé « sur papier », avec des arbres de décision[83] pour guider sa conception, et il devait ensuite être programmé.

Lors de la première étape, trois « problèmes majeurs », communs chez les internautes moyens, ont été identifiés. Chaque problème avait servi de point de départ à la création d'un arbre de décision représentant le cheminement que l'internaute devait suivre pour obtenir un diagnostic[84].

- Mon ordinateur est lent.
- Les logiciels que j'utilise gèlent souvent.
- Je rencontre certaines anomalies (par exemple, des messages d'erreur ou des comportements informatiques inhabituels).

Au cours de l'élaboration des trois arbres de décision, deux constatations ont fait surface :

- En aucun cas ce guide ne serait objectif. Les questions posées guidaient l'internaute dans un processus linéaire précis et prédéterminé par l'étudiante, ce qui était potentiellement problématique, puisque les menaces ne respectent aucun « cheminement » précis dans

[81]L'annexe 4 présente un aperçu du « guide de recherche » anticipé à l'origine.
[82]Soit dit en passant, lors de la première étape du développement de ce guide, aucune fonctionnalité comparable n'avait été trouvée sur Internet.
[83]Il s'agit d'une « représentation schématique des différentes actions séquentielles pouvant mener à la solution d'un problème, compte tenu de tous les facteurs pertinents et parfois aléatoires » (Grand dictionnaire terminologique).
[84]L'annexe 5 présente une ébauche d'un des arbres de décision créés.

leur exécution. L'exactitude du diagnostic pouvait être facilement remise en cause, ce qui pouvait contrevenir à l'utilité du site au complet.

- La manipulation de l'outil serait potentiellement complexe pour un internaute novice. S'il n'était pas en mesure de bien comprendre une question, il pouvait donner une réponse « au hasard » et, en fin de compte, obtenir un diagnostic erroné. Cette situation était très problématique, car les internautes novices font partie du public cible. L'utilité du guide, et du site en entier, pouvait alors être remise en question, sans oublier que les difficultés de manipulation pouvaient engendrer des lacunes au point de vue de l'utilisabilité.

Ainsi, le risque d'obtention d'un diagnostic inexact ou inapproprié était élevé. Le « guide de recherche » devait être repensé pour minimiser ce risque. Son développement s'est donc arrêté à la première étape, qui a fait jaillir ces difficultés, et la phase de programmation n'a jamais été entamée.

Une alternative au « guide de recherche » a par la suite été élaborée : au lieu d'avoir accès à un guide qui lui permet de cheminer une étape à la fois vers un diagnostic, l'internaute pouvait désormais consulter de l'information classée sous la forme de questions et de réponses, présentant des problèmes et leurs solutions. L'objectif de cette série de questions et réponses n'était plus de soutenir l'internaute dans une démarche pas à pas, mais de lui permettre de circuler par lui-même dans un amas de renseignements classés, adaptés et vulgarisés, et de trouver une solution à son problème.

Malgré la complétude de cette série de questions et de réponses, il lui manquait une touche de personnalisation. Le « guide de recherche » original était un outil plus personnalisé que les questions et réponses. Pour que l'aide au diagnostic soit en mesure d'offrir un certain niveau de personnalisation, une fonctionnalité complémentaire a été créée : une liste de bonnes pratiques[85] personnalisable et imprimable (décrite au point 3.2.2.1)

3.3.2.3. LE FORMULAIRE DE CONTACT

Aucun moyen de contact n'avait été prévu à l'origine. Pourtant, lors de l'élaboration du site, il s'est avéré essentiel pour répondre au critère ergonomique relatif à la correction des erreurs. En effet,

[85]Le terme « bonnes pratiques » a été modifié pour « bonnes habitudes et attitudes », puisque « bonne pratique » était déjà utilisé par l'Institut de sécurité de l'information du Québec (ISIQ) sur le site http://monidentite.isiq.ca.

si un internaute détecte une erreur due à une mauvaise programmation, une quelconque inexactitude dans le contenu du site, ou même un lien mort, il doit être en mesure de le signaler.

Un formulaire de contact a donc été créé[86]. En plus de permettre le signalement d'erreurs, il permet l'envoi de toute requête touchant aux conditions d'utilisation du site et la transmission d'un commentaire ou d'une question d'ordre général. Ce formulaire a contribué à rehausser l'utilité du site.

3.4. LA POSTPRODUCTION DU SITE

Le site a été publié le 17 septembre 2010, lorsque l'adresse URL* http://pages.usherbrooke.ca/securite_internet101/ a été activée et qu'elle a affiché la page d'accueil de *Sécurité Internet 101 : Technologie et comportement.*

La pérennité de ce genre de document, dans un univers qui évolue chaque jour, exige des mises à jour fréquentes, tel que mentionné au point 3.2.2.2. Cette dimension déborde largement du cadre du présent projet. Cependant, on remarquera que plusieurs dispositions (structure du site, classement des fichiers, programmation HTML, mécanismes de suivi du trafic sur le site[87]) ont été mises en place pour le faire. Le site étant finalisé, il est important d'en assurer la postproduction pour le faire connaître et permettre aux internautes de l'utiliser et d'en profiter. Pour y arriver, sa publication finale doit être planifiée (avec un nom de domaine* dédié), de même que sa publicisation et, d'ici quelque temps, son évaluation, autant d'éléments souhaitables, mais difficilement réalisables dans le cadre de ce mémoire production.

[86]Le formulaire de contact n'est pas accessible à partir de toutes les pages du site; on peut s'y rendre par les conditions d'utilisation. L'accès a été pensé de cette manière pour que les internautes consultent d'abord les conditions d'utilisation avant de contacter l'auteure du site. De plus, ce type d'accès pourrait limiter certains abus (pourriels, sollicitation, etc.).

[87]Le service Google Analytics permet de suivre le trafic sur le site et d'obtenir plusieurs statistiques qui faciliteront ses mises à jour (pages les plus visitées, les plus désuètes, etc.).

CONCLUSION

Ce mémoire production avait pour but d'abord de présenter l'état du média Internet, un média à l'ascension fulgurante qui offre des possibilités attrayantes pour ses utilisateurs, mais qui comporte également des risques bien réels dont l'impact peut être très sérieux, voire désastreux. Devant cette réalité, il est apparu que les internautes ne sauraient rester inactifs et qu'ils devraient acquérir quelques connaissances de base leur permettant de mieux gérer le risque, en mode proactif, ou, s'il est trop tard, de limiter l'impact des dégâts en mode réactif. Concrètement, pour y arriver, il leur faut non seulement installer des logiciels de sécurité, mais aussi, et peut-être surtout, adopter des comportements sécuritaires. Mais encore faut-il qu'ils aient accès à des ressources pertinentes pour les soutenir dans leurs démarches!

Dans l'esprit du développement d'un outil le plus efficace possible, il convenait d'examiner un échantillon caractéristique de sites Web francophones traitant de sécurité Internet, et pouvant être repérés et consultés par les internautes moyens. À la lumière des observations de cet examen, il a été établi que ces ressources sont habituellement bien intentionnées, mais qu'elles comportent des faiblesses ou lacunes aux points de vue de l'utilité et de l'utilisabilité, ce qui fondait la pertinence de la création d'un outil adapté au public des internautes moyens, et délimitait globalement le périmètre de la production dudit outil.

L'objectif du projet pouvait ensuite être formulé : mettre à la disposition des internautes un site qui rassemble, en un seul et même lieu, des définitions, des outils d'aide et des ressources supplémentaires tant pour prévenir que pour guérir. Un cadre méthodologique appuyé sur les critères ergonomiques de Dominic Scapin et Christian Bastien, de même que sur l'ouvrage *De la lettre à la page Web : Savoir communiquer avec le grand public* du Gouvernement du Québec, a été conceptualisé et constitué afin de guider l'atteinte de cet objectif et donc, de répondre au besoin en protection des internautes moyens.

Finalement, la production de l'outil anticipé dans l'objectif s'est déroulée en trois étapes, à savoir la préproduction, l'élaboration des contenus et la conception du site en soi. Bon nombre de difficultés ont fait surface et elles ont toutes été dûment documentées, de même que les changements apportés pour les solutionner. Ces changements, qu'on peut qualifier d'améliorations par rapport aux prévisions initiales du projet, avaient pour but d'assurer l'adéquation du site Web à l'objectif de recherche, de même qu'aux critères méthodologiques d'utilité et d'utilisabilité, les

deux principales composantes de l'ergonomie Web. Bref, ces modifications visaient à optimiser l'acte de communication que constitue le site Web et, ce faisant, à contribuer à instrumenter les internautes moyens.

Il va sans dire que de plus en plus d'internautes n'auront pas le choix de s'intéresser au sujet de la sécurité Internet à l'avenir, que ce soit en raison d'une difficulté personnelle ou par désir de prévention. Devant un monde virtuel en croissance constante, peuplé par les visionnaires et les dissidents, où circulent les menaces tant logicielles qu'humaines, toujours plus nombreuses, diversifiées, complexes et dangereuses, il n'auront d'autres options que de se renseigner, de se protéger et de s'adapter, sans quoi ils s'exposeront à de fâcheuses conséquences. Ils pourront toujours, souhaitons-le, se référer à l'outil conçu dans le cadre de ce projet pour obtenir l'information et l'aide requises. Cependant, dans un univers en perpétuelle mutation, cet outil devrait subir des mises à jour régulières et des évaluations périodiques pour assurer son utilité et son utilisabilité à long terme. Ainsi, les internautes auraient à leur disposition un outil fiable qui les aiderait à rester aux aguets, un geste qui pourrait peut être perçu comme « exigeant », mais qui comporte une intéressante part de récompense.

RÉFÉRENCES BIBLIOGRAPHIQUES DU MÉMOIRE

Article de périodique Internet

HUOT, François. « Discours sur l'état des menaces Internet », *Direction informatique*, [En ligne], 28 septembre 2007, http://www.directioninformatique.com/DI/client/fr/DirectionInformatique/Nouvelles.asp?id=45308 (Page consultée le 17 septembre 2010).

Document Web (en format PDF)

BUREAU DE LA PUBLICITÉ INTERACTIVE DU CANADA et ERNST & YOUNG. *2009 Actual + 2010 Estimated Canadian Online Advertising Revenue Survey*, [En ligne], 2010, http://www.iabcanada.com/reports/IABCanada_2009Act2010Budg_CdnOnlineAdRev_FINAL.pdf (Document consulté le 17 septembre 2010), 18 p.

MICROSOFT CORPORATION. *Rapport Microsoft sur les données de sécurité – volume 8 (juillet – décembre 2009)*, [En ligne], 2010, http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=2c4938a0-4d64-4c65-b951-754f4d1af0b5 (Document consulté le 17 septembre 2010), 22 p.

Extraits de sites Web

BUREAU DE LA PUBLICITÉ INTERACTIVE DU CANADA. « La publicité en ligne au Canada atteint 1,82 milliard de dollars en 2009; et 2,1 milliards sont prévus pour 2010! », *Bureau de la publicité interactive du Canada*, [En ligne], 2010, http://www.iabcanada.com/newsletters/fr_081010.shtml (Page consultée le 17 septembre 2010).

CEFRIO. « NETendances – Juillet 2009 », *Blogue du Cefrio*, [En ligne], 2009, http://blogue.cefrio.qc.ca/2009/07/netendances-%E2%80%93-juillet-2009/ (Page consultée le 17 septembre 2010).

ERGOLAB. « Les critères ergonomiques de Scapin et Bastien, Partie 1 », *Ergolab, ergonomie Web et logiciel*, [En ligne], 2 décembre 2003, http://www.ergolab.net/articles/criteres-ergonomiques-1.php (Page consultée le 17 septembre 2010).

ERGOLAB. « Les critères ergonomiques de Scapin et Bastien, Partie 2 », *Ergolab, ergonomie Web et logiciel*, [En ligne], 10 décembre 2003, http://www.ergolab.net/articles/criteres-ergonomiques-2.php (Page consultée le 17 septembre 2010).

NETCRAFT. « June 2010 Web Server Survey », *Netcraft*, [En ligne], 2010, http://news.netcraft.com/archives/2010/06/16/june-2010-web-server-survey.html (Page consultée le 17 septembre 2010).

NIELSEN, Jakob. « Usability 101: Definition and Fundamentals - What, Why, How (Jakob Nielsen's Alertbox) », *Useit.com*, [En ligne], 2008, http://www.useit.com/alertbox/20030825.html (Page consultée le 17 septembre 2010).

ORGANISATION INTERNATIONALE DE NORMALISATION (ISO). « ISO 9241-11:1998 - Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) -- Partie 11: Lignes directrices relatives à l'utilisabilité », *Organisation internationale de normalisation*, [En ligne], 1998, http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=16883 (Page consultée le 17 septembre 2010).

SANS INSTITUTE. « SANS INSTITUTE – SANS Top-20 Security Risks (2007 Annual Update) », *SANS Institute*, [En ligne], 2007, http://www.sans.org/top20/2007/, (Page consultée le 17 septembre 2010).

ZOOKNIC INTERNET INTELLIGENCE. « Geography of Internet Users », *Site de Zooknic Internet Intelligence*, [En ligne], 2008, http://www.zooknic.com/Users/index.html (Page consultée le 17 septembre 2010).

Sites Web

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION. *Portail de la sécurité informatique – ANSSI – République française*, [En ligne], 2010, http://www.securite-informatique.gouv.fr/index.html (Page consultée le 17 septembre 2010).

COMMENTCAMARCHE.NET. *Forum d'assistance informatique*, [En ligne], 2010, http://www.commentcamarche.net/forum/ (Page consultée le 17 septembre 2010).

CYBERPRESSE. *Technaute*, [En ligne], 2010, http://technaute.cyberpresse.ca/ (Page consultée le 17 septembre 2010).

DIRECTION INFORMATIQUE. *Direction informatique | technologies de l'information, TI, communications, stratégies*, [En ligne], 2010, http://www.directioninformatique.com/ (Page consultée le 17 septembre 2010.

DUMAIS, Nelson. *La chronique de Nelson*, [En ligne], 2010, http://blogues.cyberpresse.ca/technaute/dumais/ (Page consultée le 17 septembre 2010).

INTERNET 101. *Internet 101*, [En ligne], 2010, http://www.internet101.ca (Site désormais hors ligne. Site en ligne au moment de la consultation du 26 juin 2010).

INTERNET WORLD STATS. *World Internet Usage Statistics News and World Population Stats*, [En ligne], 2010, http://www.internetworldstats.com/stats.htm (Page consultée le 17 septembre 2010).

INSTITUT DE SÉCURITÉ DE L'INFORMATION DU QUÉBEC (ISIQ). *Je protège mon identité sur Internet*, [En ligne], 2009, http://monidentite.isiq.ca (Page consultée le 17 septembre 2010).

JUD, Emmanuel. *Secuser.com – Sécurité informatique et protection de la vie privée*, [En ligne], 2010, http://www.secuser.com/index.htm (Page consultée le 17 septembre 2010).

LE JARGON FRANÇAIS. *Jargonf:Accueil – Le Jargon Français 4.1 – dictionnaire d'informatique*, [En ligne], 2010, http://jargonf.org/wiki/Accueil (Page consultée le 17 septembre 2010).

LE ROUZIC, Stéphanie. *Utilisabilité.info – Les Nouvelles de l'Utilisabilité*, [En ligne], 2010, http://www.utilisabilite.info/dotclear/index.php?Normes (Page consultée le 17 septembre 2010).

NET MARKET SHARE. *Market share for browsers, operating systems and search engines*, [En ligne], 2010, http://marketshare.hitslink.com/ (Page consultée le 17 septembre 2010).

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. *Grand dictionnaire terminologique*, [En ligne], 2010, http://www.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp (Page consultée le 17 septembre 2010).

PINARD, Pierre. *Assiste.com – Sécurité informatique et protection de la Vie privée sur l'Internet*, [En ligne], 2008, http://assiste.com.free.fr/index.html (Page consultée le 17 septembre 2010).

SYMPATICO.CA. *Synchro Blogue*, [En ligne], 2010, http://www.synchro-blogue.com/ (Page consultée le 17 septembre 2010).

VARIN, Annie. *Sécurité Internet 101 : Technologie et comportement*, [En ligne], 2010, http://pages.usherbrooke.ca/securite_internet101 (Page consultée le 17 septembre 2010).

W3C. *World Wide Web Consortium (W3C)*, [En ligne], 2010, http://www.w3.org/ (Page consultée le 17 septembre 2010).

WIKIPEDIA. *Wikipedia, the free encyclopedia*, [En ligne], 2010, http://en.wikipedia.org/wiki/Main_Page (Page consultée le 17 septembre 2010).

WIKIPÉDIA. *Wikipédia, l'encyclopédie libre*, [En ligne], 2010, http://fr.wikipedia.org/wiki/Accueil (Page consultée le 17 septembre 2010).

Livres

BEAVER, Kevin. *Combattre les Hackers pour les nuls*, Coll. « Pour les nuls », Traduction de B. Jolivart et P. Escartin, Paris, Éditions First Interactive, 2004, 423 p.

BOLCH, Laurent et Christophe WOLFHUGEL. *Sécurité informatique : Principes et méthodes*, Paris, Groupe Eyrolles, 2006, 261 p.

CLERC, Isabelle et Éric KAVANAGH – GOUVERNEMENT DU QUÉBEC. *De la lettre à la page Web : Savoir comment communiquer avec le grand public*, [s. l.], Les Publications du Québec, 2006, 376 p.

GHERNOUATI-HÉLIE, Solange. *Internet et sécurité*, Coll. « Que sais-je? », Paris, Presses Universitaires de France, 2002, 126 p.

GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition*, Coll. « microapp », Paris, Micro Application, 2007, 1247 p.

JACOBI, Daniel. *La communication scientifique : discours, figures, modèeles*, Coll. « Communication, Médias et Sociétés », Grenoble, Presses Universitaires de Grenoble, 1999, 277 p.

MALAVOY, Sophie. *Guide pratique de vulgarisation informatique*, Montréal, Acfas, 1999, 38 p.

NIELSEN, Jakob et Hoa LORANGER. *Site Web : priorité à la simplicité*, Traduction de N. Le Guillou de Penanros, Paris, CampusPress, 2007, 403 p.

Périodique

Micro hebdo, n° 608 (semaine du 10 décembre au 16 décembre 2009)- , Paris, Groupe 01.

Mémoire de maîtrise

EL JAMAÏ, Yasmine. *La régulation de la propagande haineuse sur l'Internet : le cas du projet Nizkor*, Mémoire (M. A.), Université de Montréal, 2000, 140 p.

RÉFÉRENCES BIBLIOGRAPHIQUES DE LA PRODUCTION

Sites Web

AGNITUM. *Outpost Firewall Free*, [En ligne], 2010, http://free.agnitum.com/ (Page consultée le 17 septembre 2010).

ANTIPHISHING WORKING GROUP. *APWG*, [En ligne], 2010, http://www.antiphishing.org/ (Page consultée le 17 septembre 2010).

AVAST SOFTWARE A.S. *Avast! Be free*, [En ligne], 2010, http://www.avast.com/fr-fr/index (Page consultée le 17 septembre 2010).

AVIRA. *Antivirus gratuit – Avira Antivir*, [En ligne], 2010, http://www.free-av.com/fr/index.html (Page consultée le 17 septembre 2010).

BEST SECURITY TIPS. *Best Security Tips*, [En ligne], 2010, http://www.bestsecuritytips.com/ (Page consultée le 17 septembre 2010).

CLUBIC. *Clubic : Actualité informatique, Comparatifs, Logiciels et Forum*, [En ligne], 2010, http://www.clubic.com/ (Page consultée le 17 septembre 2010).

COMMENTCAMARCHE.NET. *Forum d'assistance informatique*, [En ligne], 2010, http://www.commentcamarche.net/forum/ (Page consultée le 17 septembre 2010).

CNET. *Download.com*, [En ligne], 2010, http://download.cnet.com/windows/ (Page consultée le 17 septembre 2010).

DIRECTION INFORMATIQUE. *Direction informatique | technologies de l'information, TI, communications, stratégies*, [En ligne], 2010, http://www.directioninformatique.com/ (Page consultée le 17 septembre 2010.

EQUIFAX INC. *Solutions personnelles: Dossiers de crédit, Scores de crédit, Protection contre le vol d'identité*, [En ligne], 2010, http://www.equifax.com/home/fr_ca (Page consultée le 17 septembre 2010).

FONDATION INTERNET NOUVELLE GÉNÉRATION (FING) et autres. *InternetActu.net*, [En ligne], 2010, http://www.internetactu.net/ (Page consultée le 17 septembre 2010).

FREE DOWNLOADS CENTER. *Free Downloads Center - software and free game downloads*, [En ligne], 2009, http://www.freedownloadscenter.com/ (Page consultée le 17 septembre 2010).

GENDARMERIE ROYALE DU CANADA (GRC) et autres. *PhoneBusters – Le centre d'appel antifraude du Canada*, [En ligne], 2010, http://www.phonebusters.com/francais/recognizeit_phishingemails.html (Page consultée le 17 septembre 2010).

GET SAFE ONLINE. *Get Safe Online*, [En ligne], 2010, http://www.getsafeonline.org/ (Page consultée le 17 septembre 2010).

HOAXBUSTER.COM. *HoaxBuster - Premiere ressource francophone sur les hoax*, [En ligne], 2009, http://www.hoaxbuster.com/ (Page consultée le 17 septembre 2010).

HOAXKILLER.FR. *Hoaxkiller.fr, moteur de recherche anti-hoax*, [En ligne], 2008, http://www.hoaxkiller.fr/ (Page consultée le 17 septembre 2010).

INFORMACTION. *NoScript*, [En ligne], 2010, http://noscript.net/ (Page consultée le 17 septembre 2010).

INSTITUT DE SÉCURITÉ DE L'INFORMATION DU QUÉBEC (ISIQ). *ISIQ*, [En ligne], 2009, http://www.isiq.ca/ (Page consultée le 17 septembre 2010).

INSTITUT DE SÉCURITÉ DE L'INFORMATION DU QUÉBEC (ISIQ). *Je protège mon identité sur Internet*, [En ligne], 2009, http://monidentite.isiq.ca (Page consultée le 17 septembre 2010).

INTERNET SYSTEMS CONSORTIUM. *Internet Systems Consortium*, [En ligne], 2010, https://www.isc.org/ (Page consultée le 17 septembre 2010).

INTERNET WORLD STATS. *World Internet Usage Statistics News and World Population Stats*, [En ligne], 2010, http://www.internetworldstats.com/stats.htm (Page consultée le 17 septembre 2010).

JUD, Emmanuel. *Secuser.com – Sécurité informatique et protection de la vie privée*, [En ligne], 2010, http://www.secuser.com/index.htm (Page consultée le 17 septembre 2010).

KAMINSKY, Dan. *DoxPara Research*, [En ligne], 2008, http://www.doxpara.com/ (Site temporairement inaccessible au moment de la consultation le 17 septembre 2010).

KASPERSKY LAB. *Viruslist.com - Information Sur les Virus, les Hackers et les Spams*, [En ligne], 2010, http://www.viruslist.com/fr/index.html (Page consultée le 17 septembre 2010).

LAVASOFT. *Ad-Aware by Lavasoft - Antivirus software, free spyware removal, firewall*, [En ligne], 2010, http://www.lavasoft.com/?domain=lavasoftusa.com (Page consultée le 17 septembre 2010).

LE JARGON FRANÇAIS. *Jargonf:Accueil – Le Jargon Français 4.1 – dictionnaire d'informatique*, [En ligne], 2010, http://jargonf.org/wiki/Accueil (Page consultée le 17 septembre 2010).

MALWAREBYTES. *Malwarebytes Blog*, [En ligne], 2010, http://malwarebytes.besttechie.net/ (Site temporairement hors ligne au moment de la consultation le 17 septembre 2010).

MCAFEE. *McAfee - Antivirus Software and Intrusion Prevention Solutions*, [En ligne], 2010, http://www.mcafee.com/ca-fr/?langid=48 (Page consultée le 17 septembre 2010).

MEMOCLIC. *MemoClic, cliquez utile!*, [En ligne], 2010, http://www.memoclic.com/ (Page consultée le 17 septembre 2010).

MSN.FR. *Dicos – MSN Encarta*, [En ligne], 2009, http://fr.encarta.msn.com/encnet/features/dictionary/dictionaryhome.aspx (Page consultée le 17 septembre 2010).

NARAYAN, Bharath M. *Bharath's Security Blog*, [En ligne], 2010, http://bharath-m-narayan.blogspot.com/ (Page consultée le 17 septembre 2010).

NET MARKET SHARE. *Market share for browsers, operating systems and search engines*, [En ligne], 2010, http://marketshare.hitslink.com/ (Page consultée le 17 septembre 2010).

NETMEDIA EUROPE FRANCE. *Silicon.fr*, [En ligne], 2010, http://www.silicon.fr/ (Page consultée le 17 septembre 2010).

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. *Grand dictionnaire terminologique*, [En ligne], 2010, http://www.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp (Page consultée le 17 septembre 2010).

PCWORLD COMMUNICATIONS INC. *Reviews and News on Tech Products, Software and Downloads – PCWorld*, [En ligne], 2010, http://www.pcworld.com/ (Page consultée le 17 septembre 2010).

PINARD, Pierre. *Assiste.com – Sécurité informatique et protection de la Vie privée sur l'Internet*, [En ligne], 2008, http://assiste.com.free.fr/index.html (Page consultée le 17 septembre 2010).

REASONABLE SOFTWARE HOUSE LIMITED. *Reasonable Anti-phishing*, [En ligne], 2007, http://antiphishing.reasonables.com/PhishTest.aspx?Case=2 (Page consultée le 17 septembre 2010).

SAFER NETWORKING LTD. *Spybot Search&Destroy*, [En ligne], 2010, http://www.safer-networking.org/fr/download/index.html (Page consultée le 17 septembre 2010).

SOFTPEDIA. *Free Downloads Encyclopedia – Softpedia*. [En ligne], 2010, http://www.softpedia.com/ (Page consultée le 17 septembre 2010).

SYMANTEC. *Solutions antivirus, de sécurité et de disponibilité : Symantec Corporation*, [En ligne], 2010, http://www.symantec.com/fr/ca/index.jsp (Page consultée le 17 septembre 2010).

SYMPATICO.CA. *Synchro Blogue*, [En ligne], 2010, http://www.synchro-blogue.com/ (Page consultée le 17 septembre 2010).

TRANSUNION. *TransUnion Canada*, [En ligne], 2010, http://www.transunion.ca/ca/home_fr.page (Page consultée le 17 septembre 2010).

UBM TECHWEB. *Security News brought to you by TechWeb*, [En ligne], 2010, http://www.techweb.com/security (Page consultée le 17 septembre 2010).

WHO.IS. *Who.is: Whois, Website, Domain Name, and IP Tools*, [En ligne], 2010, http://www.who.is/ (Page consultée le 17 septembre 2010).

WIKIPEDIA. *Wikipedia, the free encyclopedia*, [En ligne], 2010, http://en.wikipedia.org/wiki/Main_Page (Page consultée le 17 septembre 2010).

WIKIPÉDIA. *Wikipédia, l'encyclopédie libre*, [En ligne], 2010, http://fr.wikipedia.org/wiki/Accueil (Page consultée le 17 septembre 2010).

Extraits de site Web

AV-COMPARATIVES. « Summary Reports », *AV-Comparatives*, [En ligne], 2010, http://www.av-comparatives.org/comparativesreviews/main-tests/summary-reports (Page consultée le 17 septembre 2010).

CNET NETWORKS. « Cookie », *Internet Security Zone.com*, [En ligne], 2010, http://fr.internetsecurityzone.com/Glossary/Cookie (Page consultée le 17 septembre 2010).

CNET NETWORKS. « Logiciel espion », *Internet Security Zone.com*, [En ligne], 2010, http://fr.internetsecurityzone.com/Glossary/Spyware (Page consultée le 17 septembre 2010).

CNET NETWORKS. « Logiciel publicitaire », *Internet Security Zone.com*, [En ligne], 2010, http://fr.internetsecurityzone.com/Glossary/Adware (Page consultée le 17 septembre 2010).

EMSI SOFTWARES. « Emisoft Anti-Malware », *Emisoft*, [En ligne], 2010, http://www.emsisoft.fr/fr/software/antimalware/ (Page consultée le 17 septembre 2010).

ESET. « Scanner en ligne ESET – ESET NOD32 Antivirus 4 », *ESET*, [En ligne], 2010, http://www.eset-nod32.fr/scanner.html (Page consultée le 17 septembre 2010).

FACEBOOK. « Salle de presse, Statistiques », *Facebook*, [En ligne], 2010, http://www.facebook.com/press/info.php?statistics (Page consultée le 17 septembre 2010).

FILEHIPPO. « Download Piriform CCleaner », *Filehippo*, [En ligne], 2010, http://www.filehippo.com/download_ccleaner/ (Page consultée le 17 septembre 2010).

FUTURA-SCIENCES. « Rootkit », *Futura-Techno*, [En ligne], 2010, http://www.futura-sciences.com/fr/definition/t/internet-2/d/rootkit_4030/ (Page consultée le 17 septembre 2010).

IOBIT. « Advanced SystemCare Free Download », *Iobit*, [En ligne], 2010, http://www.iobit.com/advancedwindowscarcper.html?Str=download (Page consultée le 17 septembre 2010).

JAVACOOL SOFTWARES. « SpywareBlaster », *Javacool Softwares*, [En ligne], 2010, http://www.javacoolsoftware.com/spywareblaster.html (Page consultée le 17 septembre 2010).

MALEKAL. « Gestion des utilisateurs sous Windows », *Malekal, forum d'aide informatique*, [En ligne], 2010, http://www.malekal.com//gestion_utilisateur_windows.php (Page consultée le 17 septembre 2010).

MATOUSEC. « Proactive Security Challenge: Results and comments », *Matousec.com*, [En ligne], 2010, http://www.matousec.com/projects/proactive-security-challenge/results.php (Page consultée le 17 septembre 2010).

MICROSOFT CORPORATION. « Aide et support Microsoft », *Microsoft*, [En ligne], 16 septembre 2010, http://support.microsoft.com/?LN=fr-ca&x=17&y=12 (Page consultée le 17 septembre 2010).

MICROSOFT CORPORATION. « Microsoft Online Privacy Statement », *Microsoft*, [En ligne], 2010, http://privacy.microsoft.com/fr-ca/fullnotice.mspx (Page consultée le 17 septembre 2010).

MICROSOFT CORPORATION. « Principaux éléments de la Déclaration de confidentialité de Microsoft Online », *Microsoft*, [En ligne], 2010, http://privacy.microsoft.com/fr-ca/default.mspx (Page consultée le 17 septembre 2010).

MICROSOFT CORPORATION. « Watch out for fake virus alerts », *Microsoft Security*, [En ligne], 2010, http://www.microsoft.com/security/antivirus/rogue.aspx (Page consultée le 17 septembre 2010).

MICROSOFT CORPORATION. « Windows® Defender », *Microsoft Centre de téléchargement*, [En ligne], 2010, http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=435BFCE7-DA2B-4A6A-AFA4-F7F14E605A0D (Page consultée le 17 septembre 2010).

PANDA SECURITY. « Virus, Worms, antivirus and Security Information. », *Panda Security*, [En ligne], 2010, http://www.pandasecurity.com/homeusers/security-info/?sitepanda=particulares (Page consultée le 17 septembre 2010).

RÉSEAU ÉDUCATION-MÉDIAS. « Connaître les dangers - Pornographie », *Réseau Éducation-Médias*, [En ligne], 2009, http://www.media-awareness.ca/francais/enseignants/toile_enseignants/toute_securite_enseignants/dangers_pornographie.cfm (Page consultée le 12 décembre 2010).

SOPHOS. « Sophos Anti-Rootkit », *Sophos*, [En ligne], 2010, http://www.sophos.fr/products/free-tools/sophos-anti-rootkit.html (Page consultée le 17 septembre 2010).

TREND MICRO. « Trend Micro HouseCall », *Trend Micro*, [En ligne], 2010, http://housecall.trendmicro.com/fr/ (Page consultée le 17 septembre 2010).

VS REVO GROUP. « Revo Uninstaller Download », *VS Revo Group*, [En ligne], 2010, http://www.revouninstaller.com/revo_uninstaller_free_download.html (Page consultée le 17 septembre 2010).

VULGARISATION-INFORMATIQUE. « Forum informatique », *Vulgarisation informatique.com*, [En ligne], 2010, http://www.vulgarisation-informatique.com/forum-informatique.php (Page consultée le 17 septembre 2010).

YAHOO! QUÉBEC. « Questions et réponses, Informatique et Internet », *Yahoo! Québec*, [En ligne], 2010, http://qc.answers.yahoo.com/dir/index?link=list&sid=396545660 (Page consultée le 17 septembre 2010).

ZDNET. « Phishing vs. Pharming », *ZDNET*, [En ligne], 2005, http://www.zdnet.com/videos/whiteboard/phishing-vs-pharming/153441 (Page consultée le 17 septembre 2010).

Extrait d'émission de télévision

CAROLL, Jason. « Internet cell phone popcorn HOAX - secret revealed », *CNN [par YouTube]*, [En ligne], s. d., http://www.youtube.com/watch?v=KsoVEeJg3TY (Page consultée le 17 septembre 2010).

Articles de périodiques Internet

CAUCHON, Paul. « Mafiaboy, l'ado qui a fait tomber Yahoo!, eBay et CNN », *Le Devoir*, [En ligne], 1er novembre 2008, http://www.ledevoir.com/culture/livres/213623/mafiaboy-l-ado-qui-a-fait-tomber-yahoo-ebay-et-cnn (Page consultée le 17 septembre 2010).

CONDO, Jean-Charles. « Loi anti-pourriel Can-Spam : conclusion d'une première affaire », *Branchez-vous! Techno*, [En ligne], 12 octobre 2004, http://www.branchez-vous.com/actu/04-10/08-313901.html (Page consultée le 17 septembre 2010).

CONDO, Jean-Charles. « Mac OS X: un cheval de Troie déguisé en vidéo osée de Leighton Meester », *Branchez-vous! Techno*, [En ligne], 25 juin 2009, http://techno.branchez-vous.com/actualite/2009/06/mac_osx_un_cheval_de_troie_deg.html (Page consultée le 17 septembre 2010).

COGSWELL, Bryce et Mark RUSSIINOVICH. « RootkitRevealer v1.71 », *Windows Sysinternals, Microsoft TechNet*, [En ligne], 1er novembre 2006, http://technet.microsoft.com/fr-fr/sysinternals/bb897445%28en-us%29.aspx (Page consultée le 17 septembre 2010).

DUMAIS, Nelson. « Sachant que le pire est à venir... », *La chronique de Nelson*, [En ligne], 25 novembre 2008, http://blogues.cyberpresse.ca/technaute/dumais/2008/11/25/sachant-que-le-pire-est-a-venir/ (Page consultée le 17 septembre 2010).

GRONDIN, Alexis. « Les réseaux sociaux sont de vrais annuaires pour les cybercriminels », *01Net Pro*, [En ligne], 24 juillet 2008, http://pro.01net.com/editorial/387450/les-reseaux-sociaux-sont-de-vrais-annuaires-pour-les-cybercriminels/ (Page consultée le 17 septembre 2010).

JOHNSON, Maxime. « Conficker infecte 50 000 nouveaux PC par jour », *Branchez-vous! Techno*, [En ligne], 21 mai 2009, http://techno.branchez-vous.com/actualite/2009/05/conficker_infecte_50_000_nouve.html (Page consultée le 17 septembre 2010).

LEDUC, Christian. « Conficker se déploie progressivement », *Branchez-vous! Techno*, [En ligne], 27 avril 2009, http://techno.branchez-vous.com/actualite/2009/04/conficker_se_deploie_progressi.html (Page consultée le 17 septembre 2010).

RADIO-CANADA, AGENCE FRANCE-PRESSE, PRESSE CANADIENNE et BBC. « Une importante brèche colmatée », *Radio-Canada*, [En ligne], 10 juillet 2008, http://www.radio-canada.ca/nouvelles/societe/2008/07/09/001-faille-informatique.shtml (Page consultée le 17 septembre 2010).

TECHNAUTE. « Mafiaboy raconte son histoire », *Technaute*, [En ligne], 8 octobre 2008, http://technaute.cyberpresse.ca/nouvelles/internet/200810/06/01-26824-mafiaboy-raconte-son-histoire.php (Page consultée le 17 septembre 2010).

ITESPRESSO.FR. « Le roi du spam condamné à 47 mois de prison aux États-Unis », *ITEspresso.fr*, Traduction de l'artiche « Spam King Soloway sent down for 47 months » de VUNet, [En ligne], 24 juillet 2008, http://www.itespresso.fr/le-roi-du-spam-condamne-a-47-mois-de-prison-aux-etats-unis-22426.html (Page consultée le 17 septembre 2010).

WEBMASTER HUB. « Pharming : encore plus dangereux que le phishing! », *WebMaster Hub*, [En ligne], 18 octobre 2006, http://www.webmaster-hub.com/publication/Pharming-encore-plus-dangereux-que.html (Page consultée le 17 septembre 2010).

Documents Web en format PDF

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE). *Orientations de l'OCDE pour les politiques sur le vol d'identité en ligne*, [En ligne], 2008, http://www.oecd.org/dataoecd/51/59/40883671.pdf (Document consulté le 17 septembre 2010), 23 p.

Livres

BEAVER, Kevin. *Combattre les Hackers pour les nuls*, Coll. « Pour les nuls », Traduction de B. Jolivart et P. Escartin, Paris, Éditions First Interactive, 2004, 423 p.

CHARTON, ÉRIC. *Spywares et virus : Protégez-vous des logiciels escrocs*, Coll. « Kit Campus », Paris, CampusPress, 2005, 245 p.

GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition, C*oll. « microapp », Paris, Micro Application, 2007, 1247 p.

GRALLA, Preston. *PC Pest Control*, Sebastopol, O'Reilly Media Inc., 2005, 275 p.

KONG, Joseph. *Rootkits BSD : Mieux les comprendre pour mieux s'en protéger*, Paris, Campus Press, 2007, 148 p.

LEVINE, John R. *Sécurité Internet pour les nuls*, Paris, Éditions First Interactive, 2003, 398 p.

MITNICK, Kevin David. *L'art de la supercherie : les révélations du plus célèbre hacker de la planète*, Paris, CampusPress, 2005, 377 p.

SCHILLER, Craig A. et Jim BINKLEY, David HARLEY, Gadi EVRON, Tony BRADLEY, Carsten WILLEMS, Michael CROSS. *Botnets : The Killer Web App*, [s.l.], Syngress Publishing, Inc., 2007, 464 p.

TRABELSI, Zouheir et Henri LY. *La sécurité sur Internet*, Paris, Hermès Science Publications, 2005, 254 p.

Articles de périodiques

AZZEMOU, Sam. « La sécurité de votre PC : ce qui marche vraiment en 32 questions », n° 46, p. 38 – 46.

DUVAL, Loïc. « 12 suites de sécurité au banc d'essai », *Micro hebdo*, n° 608, 10 décembre au 16 décembre 2009, p. 20 – 27.

GRANGER, Jérôme, RODA, José et Jérôme SAIZ. « Halte aux nouveaux dangers du Web », *L'ordinateur individuel*, n° 203, mars 2008, p. 64 – 79.

PICARD, François. « Des précautions à prendre pour se protéger en ligne », *Atout Micro*, Vol. 21, nº 7, avril 2008, p. 12 – 15.

ANNEXE 1 : LE GLOSSAIRE[88]

Ce glossaire est limité aux termes utilisés dans le présent mémoire. Pour plus de détails, veuillez consulter le glossaire de la production accessible à l'adresse http://pages.usherbrooke.ca/securite_internet101/glossaire.html.

Adresse IP : Numéro divisé en quatre segments permettant d'identifier, de manière unique, les ordinateurs (clients et serveurs) connectés à Internet. Ce numéro permet également la localisation physique des ordinateurs connectés, si nécessaire.

Aide à la navigation : Élément d'un site Web ayant pour objectif de guider l'internaute lors de sa navigation et de lui fournir de l'aide pour se repérer[89]. Exemples : plan du site, champ de recherche (où l'on doit inscrire des mots-clés), etc.

Adresse URL : Adresse unique attribuée à un site Web. Une adresse URL respecte le modèle suivant : http://www.exemple.com. Dans ce modèle, la mention « http:// » fait référence au protocole utilisé et « exemple.com » est le nom de domaine.

Barre de titre : Barre située au haut de la fenêtre active affichant le nom du logiciel exécuté, le titre ou le nom du fichier utilisé, ainsi qu'une série de boutons permettant à l'usager d'interagir avec la fenêtre (réduire, agrandir, fermer).

Canular (*hoax*) : Fausse information souvent véhiculée par courriel et propagée par les internautes.

Cheval de Troie (*Trojan horse*) : Logiciel malveillant d'apparence inoffensif, mais pouvant offrir un accès direct à l'ordinateur à une tierce personne, lui permettant ainsi d'en prendre le contrôle.

Ciblage comportemental : Technique visant à augmenter l'efficacité d'une campagne publicitaire sur Internet. Elle permet d'afficher, sur l'ordinateur d'un internaute, de la publicité personnalisée selon ses besoins, ses intérêts et ses habitudes.

---

[88]L'ensemble des définitions de ce glossaire sont tirées du site *Sécurité Internet 101 : Technologie et comportement* (http://pages.usherbrooke.ca/securite_internet101/glossaire.html). Elles ont été documentées à l'aide des sources suivantes : le Grand dictionnaire terminologique (http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp), Wikipédia (http://fr.wikipedia.org/wiki/Accueil), Wikipedia (http://en.wikipedia.org/wiki/Main_Page) et le Jargon français (http://jargonf.org/wiki/Accueil).

[89]CLERC, I. et É. KAVANAGH – GOUVERNEMENT DU QUÉBEC. *De la lettre à la page Web : Savoir communiquer avec le grand public*, p. 294.

Clavardage : Activité en ligne où un internaute converse avec d'autres internautes en échangeant des messages tapés au clavier. Contrairement à un forum, où les échanges sont en temps différé (délai entre les messages), le clavardage permet une discussion en temps réel (aucun délai entre les messages).

Client : Dans une approche client-serveur, l'ordinateur client est un ordinateur « normal », celui possédé par un individu et utilisé pour demander de l'information par la formulation de requêtes auprès d'un serveur.

CSS (feuille de style) : *Cascading Style Sheet.* Feuille de style dite en cascade permettant de gérer la présentation (ou l'apparence) entre autres des documents HTML.

Cybercriminalité : Acte criminel commis avec de l'équipement informatique habituellement connecté à Internet.

Ergonomie Web : Discipline connexe de l'ergonomie visant à adapter ou à créer « des contenus et des fonctionnalités d'un site Web en vue d'en faciliter l'utilisation par ses visiteurs[90] ». L'ergonomie Web regroupe deux composantes, l'utilité et l'utilisabilité.

Espiogiciel (*spyware*) : Logiciel malveillant permettant de recueillir et de transmettre à une tierce personne des données sur les activités d'un internaute, à son insu, ce qui peut compromettre sa vie privée. En masse, les espiogiciels peuvent provoquer différents « malaises » informatiques, tels que des ralentissements ou un dysfonctionnement.

Faille (ou vulnérabilité) : Défaut dans un logiciel permettant une manipulation imprévue, comme l'infiltration d'un logiciel malveillant.

Faux logiciel de sécurité (*rogue*) : Logiciel malveillant ayant l'apparence d'un logiciel de sécurité légitime, mais affichant de faux avis et de faux résultats. Il s'installe souvent à la suite d'un clic imprudent sur une publicité trompeuse, ou à la suite d'une visite sur un site piégé. Il peut ensuite afficher plusieurs alertes pour inciter l'internaute à procéder à un téléchargement ou à payer pour obtenir « réparation ».

Fenêtre pop-up : Fenêtre secondaire non sollicitée qui s'affiche devant la fenêtre du navigateur et qui peut présenter de la publicité.

Fil d'Ariane : Suite de titres, « chacun représentant une subdivision de la carte du site, qui donne à l'internaute un aperçu du chemin parcouru et lui permet de repérer facilement sa position dans l'arborescence du site Web visité[91] ».

---

[90] *Grand dictionnaire terminologique*, « Ergonomie Web », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.

[91] *Grand dictionnaire terminologique*, « Fil d'Ariane », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.

Forum : Espace virtuel, souvent une page Web, où plusieurs internautes discutent de sujets en tous genres. Les échanges se font en temps différé (délai entre les messages), contrairement au clavardage* où les échanges sont en temps réel (aucun délai entre les messages).

Fraude psychologique (ingénierie sociale) : Ensemble de moyens utilisés par un fraudeur pour tromper et manipuler un individu. L'objectif est de l'inciter à commettre des actions ou à remettre de l'information confidentielle pour permettre au fraudeur de s'introduire illégalement dans un système, qu'il s'agisse du réseau d'une entreprise, du compte de banque d'un individu ou de tout autre système.

FTP : *File Transfer Protocol.* Protocole permettant le transfert de fichiers d'un ordinateur client vers un serveur et vice versa.

Hameçonnage (*phishing*) : Technique d'attaque par courriel où un fraudeur usurpe l'apparence d'une entreprise ou d'une organisation de confiance pour recueillir des renseignements confidentiels non pas en les volant, mais en incitant un internaute à les remettre de lui-même.

Historique de navigation : Fichier où sont sauvegardées toutes les adresses des pages Web visitées dans une période donnée (hebdomadairement, au cours du mois, etc.).

HTML : *Hypertext Markup Language.* Langage de balisage hypertexte qui permet la création de pages Web pouvant être visionnées à l'aide d'un navigateur.

HTTP : *Hypertext Transfer Protocol.* Protocole permettant l'affichage des pages Web (et autres contenus Web) dans un navigateur.

IMAP : *Internet Message Access Protocol.* Protocole de messagerie électronique permettant la réception (et plus précisément, la consultation) des courriels.

Infobulle : « Élément d'un système d'aide contextuelle qui, à la demande de l'utilisateur, affiche de l'information[92] » complémentaire.

Internet : Réseau international reliant des réseaux nationaux, qui peuvent communiquer entre eux grâce au protocole TCP* / IP*.

IP : *Internet Protocol.* Protocole qui donne à chaque ordinateur (client* ou serveur) la possibilité de se connecter à Internet avec une adresse unique (adresse IP*) pour rendre les échanges possibles.

Javascript : Langage de script, développé par Netscape et simplifié pour les utilisateurs débutants, servant à apporter du dynamisme aux pages Web.

---

[92] *Grand dictionnaire terminologique*, « Infobulle », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.

Langage : Dans un contexte informatique, il s'agit d'un « ensemble organisé de symboles, de mots-clés, de caractères et de règles (instructions et syntaxe) utilisé pour adresser des commandes à l'ordinateur et assurer la communication avec la machine[93]. »

Logiciel antiespiogiciels : Logiciel de sécurité visant à détecter et, si possible, à éliminer les espiogiciels et, dans certains cas, les logiciels publicitaires, les témoins traceurs et les chevaux de Troie.

Logiciel antivirus : Logiciel de sécurité visant à détecter l'intrusion de certains parasites (dont les virus, les vers informatiques et les chevaux de Troie), à les neutraliser et si possible, à les éliminer.

Logiciel de courriel : Logiciel qui permet à un internaute de recevoir, de lire, de composer et d'envoyer des courriels. Il facilite également la gestion d'un ou de plusieurs comptes courriel.

Logiciel « de rechange » : De nos jours, les logiciels utilisés massivement (peu importe leur type : traitement de texte, lecteur de musique, navigateur, etc.) sont une cible de choix pour les pirates. Dans une attaque de grande envergure, les logiciels malveillants doivent pouvoir infiltrer le plus d'ordinateurs possible. Ils cibleront alors un logiciel populaire, installé sur la majorité des ordinateurs, et l'utiliseront comme porte d'entrée en exploitant l'une de ses failles. En possédant des logiciels moins connus, souvent gratuits et en plus, très efficaces, un internaute réduit le risque d'attaque.

Logiciel publicitaire (*adware*) : Logiciel qui affiche, diffuse ou télécharge du matériel publicitaire sur un système en utilisant des renseignements par un internaute ayant donné son consentement (implicitement ou non). Les logiciels publicitaires peuvent ralentir le fonctionnement normal d'un ordinateur.

Ordinateur Mac : Ordinateur personnel utilisé par un individu à des fins personnelles ou liées au travail. Fait opposition aux ordinateurs PC.

Ordinateur PC : Ordinateur personnel utilisé par un individu à des fins personnelles ou liées au travail. Fait opposition aux ordinateurs Mac.

Navigateur : Logiciel permettant la consultation et l'exploration du *World Wide Web*. Il prend en charge la consultation de moteurs de recherche, d'applications Web, de sites Web, etc., tout en permettant à l'internaute d'interagir avec les contenus (texte, audio, vidéo, etc.).

Nom de domaine : Équivalence alphabétique d'une adresse IP. Il s'agit d'une série de caractères identifiant le nom d'un site Web et son domaine (.com, .ca, .fr, etc.) dans une adresse URL.

---

[93] *Grand dictionnaire terminologique*, « Langage », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.

Pare-feu : Dispositif de sécurité permettant de protéger un ordinateur (ou un réseau) connecté à Internet en filtrant les données qui entrent et qui sortent de l'ordinateur. Il agit comme une sorte de « barrière coulissante » pour bloquer les tentatives d'intrusions en provenance d'Internet tout en laissant passer les données fiables, et comme une sorte de « douanier » pour contrôler les données qui sont envoyées vers Internet.

***Pharming* :** Technique malveillante visant à détourner vers des sites factices des adresses URL menant habituellement à des sites légitimes.

PHP : *Hypertext Preprocessor.* Langage de script permettant la création de pages Web dynamiques pouvant être visionnées avec un navigateur.

Pirate : « Personne qui parvient illégalement ou sans autorisation à accéder à un système informatique ou à une partie de celui-ci[94]. »

Plantage : Situation où un logiciel s'interrompt de manière soudaine et inattendue.

Plugiciel : Élément logiciel complémentaire qui se greffe à un logiciel principal pour offrir une fonctionnalité supplémentaire. Une fois installé (ou mis à jour), le plugiciel interagit avec le logiciel principal sans que l'utilisateur n'ait à intervenir.

POP3 : *Post Office Protocol Version 3.* Protocole de messagerie électronique permettant la réception (et plus précisément, la récupération) des courriels.

Port : Connexion virtuelle entre Internet et un ordinateur (client ou serveur) permettant la circulation des données. On peut le comparer à une petite porte qui s'ouvre et se ferme au besoin. Lorsqu'il y a un certain contrôle de la circulation des données, on peut dire qu'un port est sécurisé.

Pourriel (*spam*) : Courriel non sollicité, souvent publicitaire et envoyé massivement, habituellement destiné à la poubelle.

Protocole : « Ensemble des spécifications décrivant les conventions et les règles à suivre dans un échange de données[95]. » Il existe des protocoles pour le courriel (POP3*, IMAP*, SMTP*), pour le Web (HTTP), pour le transfert de fichiers (FTP*), etc.

Refus de service : État d'un système, d'un serveur, d'un ordinateur ou d'un site Web où il n'est plus en mesure de fonctionner, puisqu'il ne peut plus répondre aux commandes des utilisateurs. Habituellement, le refus de service résulte d'une attaque ciblée.

---

[94] *Grand dictionnaire terminologique*, « Pirate informatique », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.

[95] *Grand dictionnaire terminologique*, « Protocole », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.

Réseau social : Site permettant à ses membres de se bâtir un réseau de contacts à des fins personnelles ou professionnelles. Chaque membre est invité à se créer un profil (plus ou moins élaboré, selon le site) et à y publier différents renseignements (texte, photo, vidéo, etc.) qui pourront être consultés par les gens composant son réseau de contacts et parfois, par un plus grand nombre de personnes encore (selon les paramètres de confidentialités établis par le membre concerné).

Exemples de réseaux sociaux : Facebook, Twitter, LinkedIn, MySpace, etc.

Rustine de sécurité : Les concepteurs des logiciels développent des correctifs de sécurité pour colmater les failles dans leurs applications dès qu'elles sont découvertes. Des avis sont alors envoyés aux utilisateurs pour qu'ils téléchargent et installent ces rustines.

Saisie d'écran : « Copie totale ou partielle de l'image affichée à l'écran d'un ordinateur[96]. »

Serveur : Dans une approche client-serveur, le serveur est un « super » ordinateur (ou un logiciel, dans le cas des serveurs virtuels) qui fournit un service en exécutant, entre autres, des requêtes formulées par des clients.

Signature d'infection : Les logiciels malveillants sont conçus avec plusieurs lignes de code. Parmi tout ce code se trouve une série de caractères propre à un seul logiciel malveillant; il s'agit de la signature.

SMTP : *Simple Mail Transfer Protocol.* Protocole de communication permettant l'envoi des courriels.

Système d'exploitation : Logiciel de base en charge de la liaison entre les ressources matérielles d'un ordinateur (carte mère, micro-processeur, disque dur, carte vidéo, etc.), les différents logiciels installés et les périphériques à l'extérieur de l'ordinateur (imprimante, écran, scanneur, etc.). Bref, il offre à l'utilisateur un environnement convivial pour manipuler son ordinateur.

TCP : *Transmission Control Protocol.* Protocole qui établit les connexions et contrôle la transmission des données. La paire TCP/IP est nécessaire à toute connexion Internet.

Témoin traceur (*tracking cookie*) : Petit fichier texte contenant de l'information sur un internaute et sur ses activités sur un site. Il peut être partagé entre plusieurs sites, à l'insu de l'internaute concerné.

---

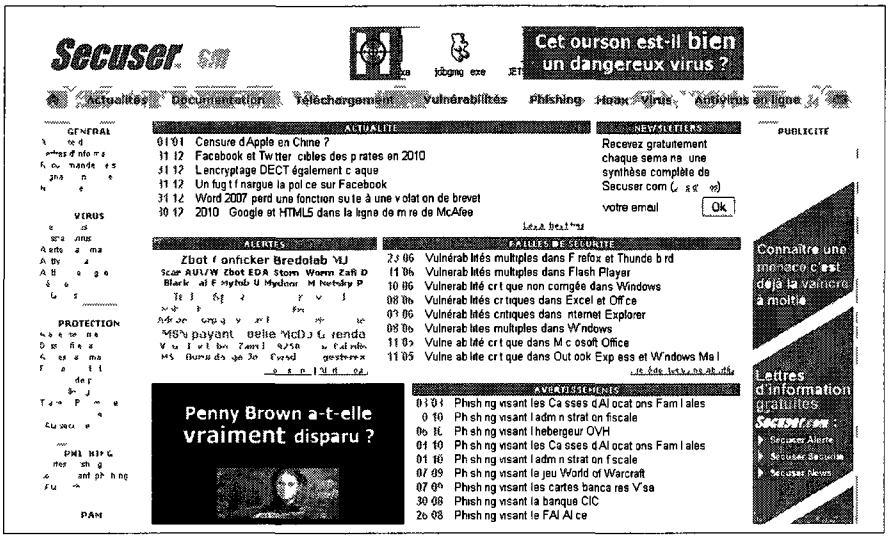
[96] *Grand dictionnaire terminologique*, « Saisie d'écran », http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp.

Trousse administrateur pirate (*rootkit*) :	Logiciel malveillant, ou ensemble de logiciels malveillants, permettant à un individu d'accéder au cœur du système infecté, tout en cachant les traces de sa présence. Il peut alors s'octroyer les privilèges d'administrateur et agir comme bon lui semble.
Utilisabilité :	Dans le contexte de l'ergonomie d'un site Web, il s'agit des « caractéristiques de qualité liées à la facilité de se servir[97] » du site en question.
Utilité :	Dans le contexte de l'ergonomie d'un site Web, il s'agit de l'état d'un site où il est en mesure de répondre aux besoins et aux attentes de ses utilisateurs (en termes de contenus).
Variante :	Logiciel malveillant conçu à partir du code d'un autre logiciel malveillant existant. Cette modification du code original permet d'ajouter de nouvelles propriétés à la variante.
Ver informatique (*worm*) :	Logiciel malveillant autonome circulant dans les réseaux et provoquant le dysfonctionnement ou le plantage d'un système.
Virus :	Logiciel malveillant ayant la possibilité de se reproduire et nécessitant, pour y arriver, l'exécution d'un programme. Les virus peuvent provoquer le dysfonctionnement ou le plantage d'un système.
Vol d'identité :	Fraude où un criminel s'empare des renseignements confidentiels d'un individu, contre son gré et généralement à son insu, afin de les utiliser à des fins illégales en se faisant passer pour l'individu lésé.
Web :	Système sur Internet qui permet de chercher de l'information et de la consulter.

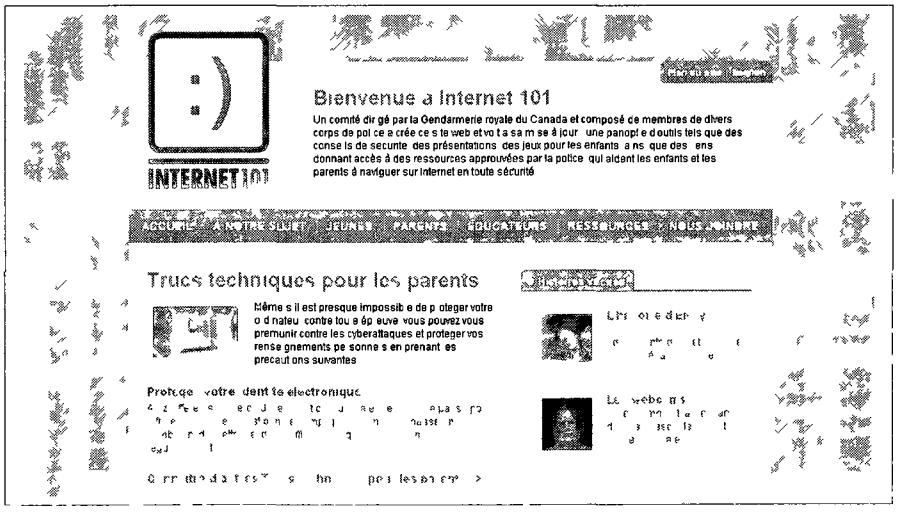
[97]NIELSEN, J. et H. LORANGER. *Site Web : priorité à la simplicité*, Paris, CampusPress, 2007, p. XVI.

ANNEXE 2 : LES SAISIES D'ÉCRAN DES SITES DE L'ÉCHANTILLON DE L'EXAMEN DES RESSOURCES EXISTANTES

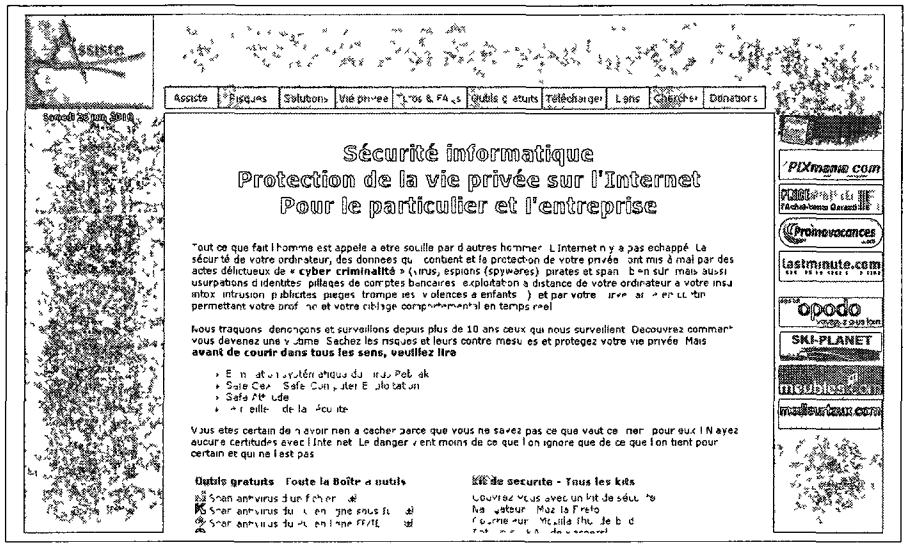
Secuser.com (http://www.secuser.com)



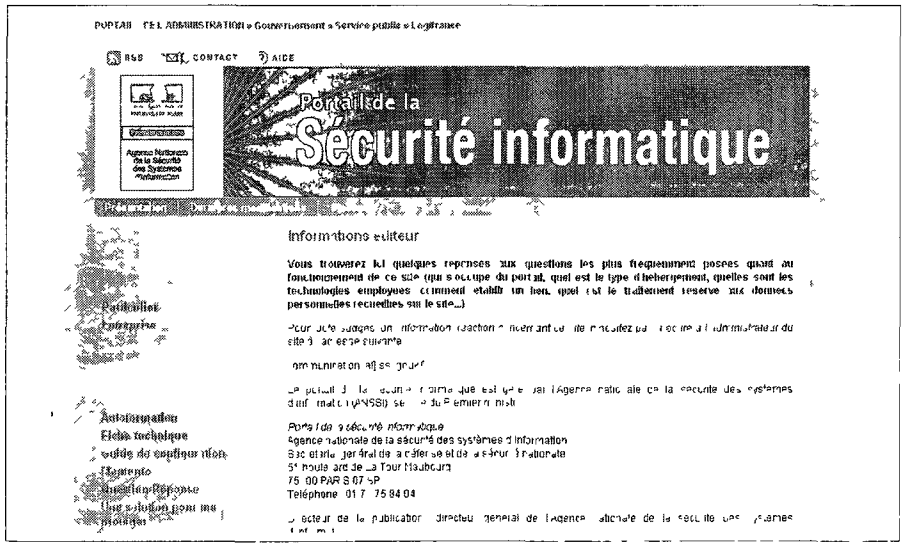
Internet 101 (http://www.internet101.ca, désormais hors ligne)



Assiste (http://http://assiste.com.free.fr)



Le portail de la sécurité informatique (http://www.securite-informatique.gouv.fr/index.html)



ANNEXE 3 : LA STRUCTURE FINALE DU SITE

- Accueil
  - Historique
  - Objectif
- Glossaire
- Menaces
  - Logiciels malveillants
    - Cheval de Troie
    - Espiogiciel
    - Faux logiciel de sécurité
    - Logiciel publicitaire
    - Rootkit
    - Ver informatique
    - Virus
  - Autres fraudes et tromperies
    - Canular
    - Hameçonnage
    - Pharming
    - Pourriel
    - Témoin traceur
- Aide au diagnostic
  - Questions et réponses
    - Urgentes
    - Moyennement urgente
    - Non urgentes
  - Liste personnalisée de bonnes habitudes et attitudes
- Faits divers
  - Vie privée
    - Bien choisir son mot de passe
    - Facebook
    - Protéger sa vie privée sur Internet
  - Internet
    - Botnet
    - Fonctionnement du DNS
    - Indicateurs de sites factices
    - Pirates Internet
  - Windows
    - Désinstaller un logiciel
    - Gestion du pare-feu Windows
    - Mises à jour
    - Mode sans échec
    - Restauration de système
- Liens
  - Ressources
  - Télécharger

ANNEXE 4 : UN EXEMPLE DU « GUIDE DE RECHERCHE » INITIAL

Étape 1 :

Que cherchez-vous?

❍ Je veux **prévenir** les menaces, donc je veux de l'information.

⊙ J'ai des **problèmes** et je cherche de l'aide. **(passage à l'étape 2)**

Étape 2 : Si vous connaissez le nom de la menace, inscrivez-le ici : [ ] OK

Si vous ne le connaissez pas, cochez l'option qui ressemble le plus à votre problème :

❍ Je reçois beaucoup de courriels non sollicités.

❍ Plusieurs fenêtres publicitaires s'affichent sur mon écran.

⊙ Mon ordinateur est « lent ». **(passage à l'étape 3)**

❍ Mon ordinateur « gèle » et je dois le redémarrer pour pouvoir l'utiliser.

❍ Je reçois souvent des messages d'erreur de la part de mon ordinateur.

❍ Mon ordinateur ne fonctionne plus du tout.

Étape 3 :

Veuillez cocher la ou les affirmations qui correspondent le mieux à votre situation :

☐ Je télécharge des logiciels (jeux, utilitaires, etc.) à partir de sites de confiance.

☐ Je télécharge de la musique à partir d'un logiciel *peer-to-peer* (exemples : LimeWire, KaZaA).

☑ Je visite des sites de divertissement où il y a beaucoup de publicité (exemple : Facebook).

☑ Je ne sais pas ce qu'est un antiespiogiciel (*Anti-Spyware*).

Passage à l'étape 4

☑ Je ne sais pas ce qu'est un pare-feu (*Firewall*).

Étape 4 :

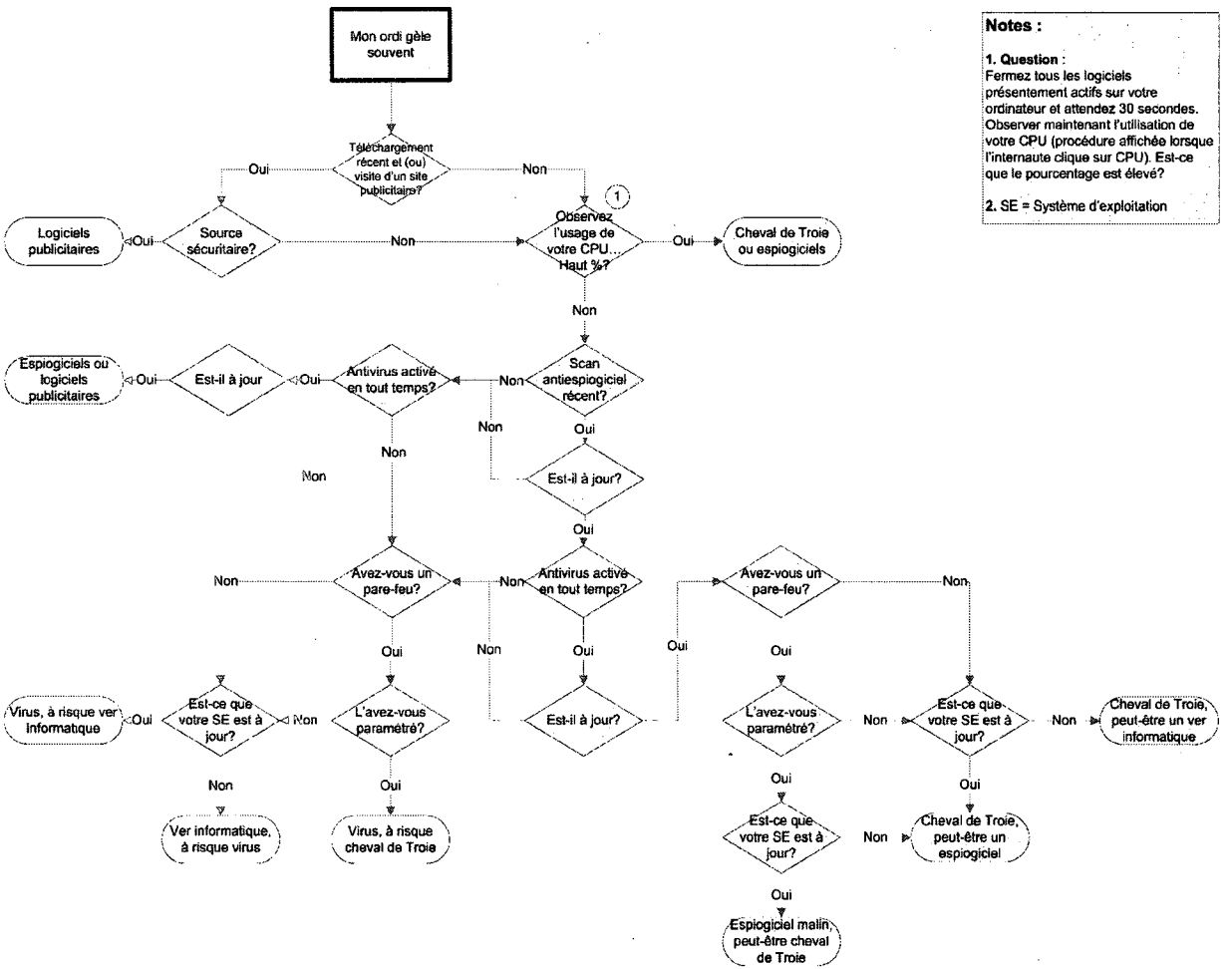
Vous êtes probablement victime d'un ou de plusieurs **espiogiciels**, ou d'un **logiciel publicitaire**.

Espiogiciel : Fiche descriptive

Logiciel publicitaire : Fiche descriptive

ANNEXE 5 : UN ARBRE DE DÉCISION DU « GUIDE DE RECHERCHE » ANTICIPÉ DANS LE PROJET ORIGINAL

Une ébauche d'un arbre de décision créé pour le « guide de recherche ». Il représente le cheminement que l'utilisateur aurait parcouru pour répondre au problème « Les logiciels que j'utilise gèlent souvent ».



ANNEXE 6 : LE SITE WEB *SÉCURITÉ INTERNET 101 : TECHNOLOGIE ET COMPORTEMENT*

Ci-joint la version imprimée du site Web au cœur de la présente production.

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

ACCUEIL

« Si Internet constitue quelquefois un jardin de roses, il ne faut pas oublier qu'il comporte des épines*. » En effet, qu'on le veuille ou non, l'agrément et le risque se côtoient régulièrement sur le réseau

L'agrément est bien connu de tous, mais qu'en est-il du risque? Parfois banalisé, parfois exagéré, il n'en demeure pas moins réel et surtout, omniprésent.

Les menaces sur Internet n'ont pas nécessairement l'apparence d'une grosse « bibitte » velue et assoiffée de malveillance ni celle d'un arnaqueur doré leurrant des portefeuilles; plusieurs font preuve d'une grande subtilité et de sournoiserie. Peu importe leur nature, elles peuvent toutes entraîner des conséquences irritantes, fâcheuses ou même catastrophiques.

« Ah! Mais j'ai un logiciel antivirus, je suis bien protégé! », serez-vous tenté de répondre. C'est un début, mais il est nettement insuffisant. Plus que jamais, les internautes doivent avoir dans une main une série de logiciels de sécurité et dans l'autre, une liste de comportements sécuritaires, pour ensuite apprendre à les combiner judicieusement. L'objectif ultime est de se protéger contre les menaces qui ciblent quincaillerie, portefeuille et identité.

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet
Maîtrise en études françaises, cheminement communication et langages
Université de Sherbrooke, 2011

Sécurité Internet 101 >> Accueil - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

http //pages usherbrooke ca/securite_internet101/

Les plus visités BDI

Sécurité Internet 101 >> Accueil

SÉCURITÉ INTERNET 101

Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Un peu d h stoire
Object f du s te
Note ir portante

ACCUEIL

Ce site propose de l'information pour prevenir et idealement guerir les problèmes technologiques liés à l'utilisation d'Internet ce qui inclut la protection des données confidentielles des internautes, et il se concentre sur cet objet avec exclusivité Les problèmes de nature « sociale » occasionnés en tout ou en partie, par Internet (cyberdépendance violence pornographie etc) ne font pas partie des sujets traités

De plus, il ne concerne que la sécurité des ordinateurs et de leurs utilisateurs lorsqu'il y a utilisation d'Internet La sécurité des appareils mobiles tels que les téléphones intelligents et les tablettes électroniques n'est pas abordée

Finalement toute mention d'ordre technologique dans ce site fait référence à la plateforme Windows en raison de la forte majorité d'internaute employant ce système d'exploitation

L objectif ultime est de se protéger contre les menaces qui ciblent quotidiennement portefeuille et identité

roses il ne faut pas oublier qu l comporte non l agrement et le risque en découlent

y a-t-il du risque? Parfois banal se parfois ut omnipresent

ment l apparence d une grosse bibitte arnaqueur doré leurrant des portefeuilles de sournoiserie Peu importe leur nature quences irritantes facheuses ou même

protégé! » serez vous tenté de répondre t Plus que jamais les internautes doivent de sécurité et dans l autre une liste de *prendre à les combler judicieusement*

Accueil Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Terminé

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Un peu d'histoire

Les années 60

Lors de ses débuts, le réseau des réseaux était petit, modeste et il ne s'appelait pas « Internet », mais bien « ARPANET ». Projeté en 1966 et mis en opération en 1969 par l'armée américaine, ARPANET était de petite envergure, mais laissait entrevoir plusieurs possibilités, puisqu'il arrivait à connecter quatre universités américaines et permettait aux ordinateurs ainsi liés de communiquer entre eux malgré la distance.

Un mythe subsiste à l'effet que le réseau ARPANET, développé en pleine Guerre froide, ait été créé pour offrir une communication militaire en cas attaque nucléaire... En réalité, il a plutôt été créé pour mettre en place un mode de connexion unique et à distance entre plusieurs ordinateurs de marques différentes.

De 1970 aux années 2000

Au cours des années 70, le réseau ARPANET a poursuivi son ascension et a enregistré plusieurs réussites. En plus de s'étendre vers d'autres continents, il a entre autres introduit le courriel et les forums de discussion. Ces deux nouveaux canaux communicationnels, bien que sommaires, étaient très prometteurs et l'avenir a su le prouver, puisqu'ils sont toujours utilisés de nos jours.

Au début des années 80, le premier protocole permettant le transfert de données sur Internet (TCP/IP) a fait son apparition, ce qui rendait le réseau de plus en plus attrayant pour les institutions et les individus à travers le monde. On offrait la chance non seulement de se connecter et de communiquer, mais également de transférer et de partager des fichiers. Fort de ces succès, le réseau a poursuivi son expansion et en 1989, il connectait 100 000 ordinateurs.

C'est ainsi qu'à l'aube des années 90, le réseau « ARPANET », désuet puisqu'il ne suffisait plus à la tâche, a complètement disparu pour laisser place à son successeur, Internet. Le *World Wide Web* a ensuite été mis en place et les populations, intriguées, ont répondu à l'offre, ce qui a fait grimper la demande. Devant un tel engouement, la création d'un navigateur à interface graphique conviviale s'imposait, d'où l'arrivée de *Mosaic*, le tout premier navigateur Web. En 1996, avec 10 millions d'ordinateurs connectés et autant d'internautes fascinés, Internet faisait ses premiers pas en tant que média « grand public ».

De 1992 à 2010, le nombre d'internautes est ainsi passé de 1 million à 1,7 milliard. Uniquement entre 2000 et 2009, la population internaute a littéralement explosé avec une augmentation de 380 %.

Aujourd'hui, en 2011

Nous verrons les chiffres poursuivre leur ascension en 2011. Mais plus d'internautes, plus d'avancement et plus de possibilités impliquent immanquablement plus de risques.

Internet va maintenant bien au-delà de la simple communication d'un message d'un émetteur à un récepteur. Plus que jamais, les internautes peuvent développer leur message, multiplier la quantité de récepteurs et se confondre dans l'anonymat, en plus de pouvoir créer du contenu, rassembler de l'information... et se faire attaquer.

Aussi désolant que cela puisse paraître, la hausse du risque va de pair avec la progression constante des possibilités technologiques. Plus il y a de latitude, plus il y a de menaces.

Pourtant, l'évolution continue et elle n'est pas prête de s'arrêter. Les risques changeront et les internautes n'auront pas le choix de s'adapter régulièrement, sans quoi ils pourraient subir de fâcheuses conséquences...

Mais les merveilles d'Internet compensent largement pour tous les efforts fournis, vous ne trouvez pas?

Sources documentaires

- Internet World Stats
- Wikipédia (français)
- Wikipedia (anglais)

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Objectif du site

Grâce à ses caractéristiques uniques par rapport aux médias de masse traditionnels (dont l'ouverture sur le monde, disponibilité constante, bilatéralité des échanges), Internet est devenu, au fil du temps, de plus en plus populaire. Cette popularité s'est traduite par un accroissement de sa complexité, une sorte de « spirale inflationniste » qui le rend malgré tout encore plus « alléchant » pour les internautes, une clientèle de plus en plus hétérogène dont une bonne partie peut se laisser complètement « hypnotiser » par le média.

À une époque où les menaces sont non seulement plus nombreuses, mais aussi (et surtout) potentiellement beaucoup plus lourdes de conséquences, il importe que les internautes se prennent en main. Pour ce faire, ils peuvent se tourner vers toutes sortes d'ouvrages qui sont souvent bien intentionnés, mais pas nécessairement utilisables pour plusieurs raisons : surenchère de contenus, faible niveau de vulgarisation et d'adaptation, utilisation d'un vocabulaire informatique parfois hermétique, etc.

L'objectif de ce site est donc d'instrumenter les internautes en leur fournissant, dans un seul et même lieu, des explications claires et abordables couvrant les menaces les plus courantes, des définitions, des outils interactifs et des ressources accessibles (logiciels, organismes à consulter, etc.), certains axées sur la perspective préventive, d'autres sur la cure.

L'objectif peut alors se résumer dans l'équation suivante :

Popularité croissante d'Internet + Complexité en hausse d'Internet + Comportements des internautes + Quantité de menaces en hausse − Documentation compréhensible et réponses accessibles pour le « grand public » = Besoin : outiller les internautes

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

GLOSSAIRE

Liste des sources documentaires:

- Grand dictionnaire terminologique
- Le Jargon français
- Wikipédia (français)
- Wikipedia (anglais)
- MSN Encarta
- Assiste.com
- InternetACTU.net
- Who.is (anglais)
- PC World (anglais)
- Softpedia (anglais)
- Memoclic
- *Le Petit Robert, dictionnaire de la langue française*, édition de 1993.

< - Page precedente

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

GLOSSAIRE

Veuillez prendre note que les sources documentaires sont indiquées pour chaque définition inscrite dans ce glossaire. Pour avoir accès à la liste complète de ces sources, cliquez ici.

Adresse IP : Numéro divisé en quatre segments permettant d'identifier, de manière unique, les ordinateurs (clients et serveurs) connectés à Internet. Ce numéro permet également la localisation physique des ordinateurs connectés, si nécessaire.

CULTURE GÉNÉRALE

Si vous croyez être anonyme sur Internet, votre adresse IP est là pour prouver le contraire

Exemple d'adresse IP : 192.168.1.101

Anglais : *IP Address*

Sources : Grand dictionnaire terminologique, Wikipédia, Who.is.

Adresse URL : Adresse unique attribuée à un site Web.

Une adresse URL respecte le modèle suivant : http://www.exemple.com. Dans ce modèle, la mention « http:// » fait référence au protocole utilisé et « exemple.com » est le nom de domaine.

Anglais : *URL Address*

Source : Grand dictionnaire terminologique

Agent logiciel : Petit logiciel autonome qui circule dans un ordinateur pour effectuer des tâches complexes ou répétitives.

Exemple de tâche répétitive : référencement de données

Anglais : *Software Agent*

Sources : Grand dictionnaire terminologique, Wikipedia

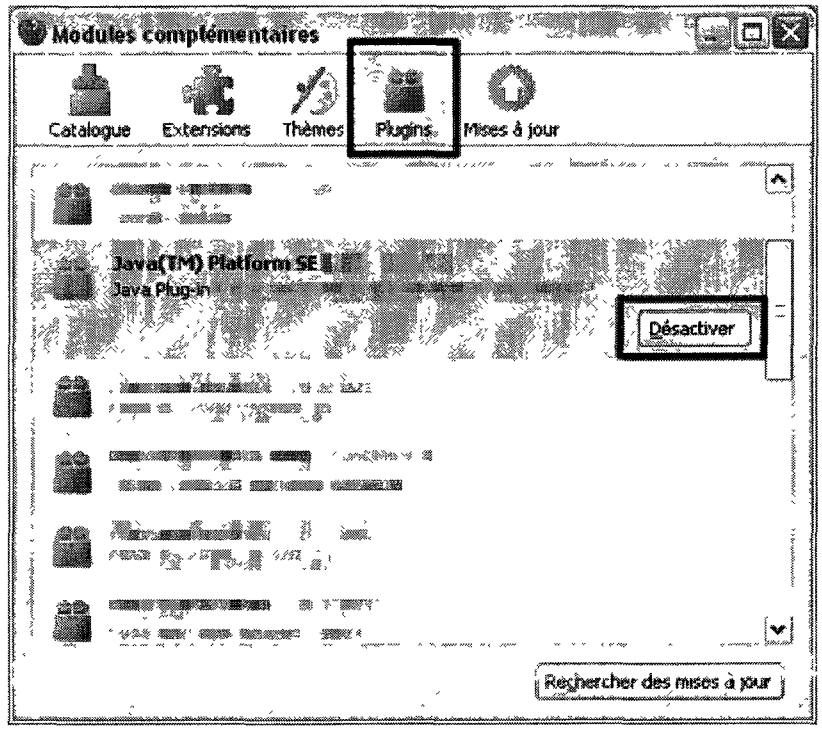
Applet Java : Petit programme intégré dans une page Web pour offrir un certain

dynamisme par l'exécution d'actions (afficher un diaporama automatique, présenter un menu interactif, etc.).

Certains applets Java malveillants peuvent exécuter des actions malicieuses, comme le téléchargement de logiciels malveillants. Il est donc important de configurer adéquatement son navigateur.

Dans le navigateur Firefox, le déclenchement de Java, essentiel à l'activation de l'applet, est automatique. Pour le désactiver (ou l'activer), voici la procédure à suivre :

1. Accéder au menu Outils/Modules complémentaires;
2. Cliquer sur l'onglet Plugins;
3. Repérer « Java(TM) Platform »;
4. Cliquer sur le bouton Désactiver (ou Activer).



Anglais : *Java Applet*

Sources : Grand dictionnaire terminologique, Le Jargon français

Application Web : Application présentée aux internautes sur un site Web et logée sur un serveur Web.

L'application ne sera jamais téléchargée; elle est sur un serveur Web et l'internaute l'utilise par l'intermédiaire d'un site Web. On peut comparer l'application Web à une émission de télévision : vous voyez l'émission (application Web) sur votre téléviseur, tout en sachant qu'elle est diffusée à partir d'une station de télé (serveur Web).

L'application permet d'exécuter aisément plusieurs tâches, comme le ferait un logiciel.

Exemple d'applications Web : Google Docs, application de gestion des photos sur Facebook, etc.

Anglais : *Web application*

Sources : Grand dictionnaire terminologique, Wikipédia.

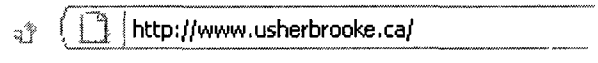
Attaque par saturation : Attaque qui vise à saturer un serveur ou un site Web en lui envoyant un très grand nombre de requêtes ou des requêtes « piégées » qu'il n'est pas en mesure de résoudre. Ainsi saturée, la cible ne sera plus en mesure de fonctionner adéquatement. S'il y a plantage, on parle alors d'un refus de service.

Synonymes : Attaque par refus de service, attaque par déni de service
Anglais : *Saturation attack, Denial of service attack*

Sources : Grand dictionnaire terminologique, Wikipédia.

Barre d'adresse : Barre horizontale située dans le haut du navigateur où est affichée l'adresse URL d'une page Web.

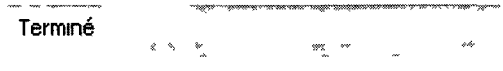
Si l'on souhaite accéder à un site Web, on doit y inscrire son adresse URL.



Anglais : *Address bar*

Sources : Grand dictionnaire terminologique

Barre d'état : Barre horizontale située au bas de la fenêtre d'un logiciel qui affiche l'activité en cours.



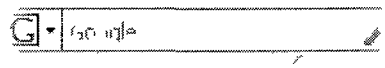
Anglais : *Status bar*

Source : Grand dictionnaire terminologique

Barre de recherche : Barre d'un moteur de recherche intégrée à un navigateur. Elle comporte une zone de texte où l'internaute peut inscrire des mots-clés s'il veut effectuer une recherche.

Par exemple, le navigateur Mozilla Firefox offre une barre de recherche

Google.



Certaines barres offrent plusieurs fonctionnalités allant au-delà de la simple recherche; on parle alors de barres d'outils. Elles sont offertes en téléchargement sur des sites Web ou lors de l'installation de logiciels. Les fonctionnalités qu'elles offrent sont diversifiées : recherche, accès à des sites précis, détection de logiciels malveillants, protection antihameçonnage, etc.

Certaines barres de recherche / barres d'outils ont toutefois des objectifs malicieux : télécharger des logiciels malveillants, voler des renseignements, etc.

Exemples : Barre d'outils et barre de recherche Google (fiables), barre d'outils Yahoo! (fiable), barre de recherche CoolWebSearch (malveillante)

Si vous installez une barre de recherche / barre d'outils, assurez-vous qu'elle provient d'une source fiable. Si vous remarquez qu'une telle barre d'outils a été installée sans votre consentement, veillez à la désinstaller.

Pour en savoir plus sur la désinstallation, consultez la fiche Désinstaller un logiciel sous Windows.

Anglais : *Search Bar*; *Tool bar*

Sources : Grand dictionnaire terminologique, Wikipédia

Barre de titre : Barre située au haut de la fenêtre active affichant le nom du logiciel exécuté, le titre ou le nom du fichier utilisé, ainsi qu'une série de boutons permettant à l'usager d'interagir avec la fenêtre (réduire, agrandir, fermer).

Source : Grand dictionnaire terminologique

Base de registre : Base de données, dans un ordinateur équipé de Windows, où sont enregistrés tous les paramètres de configuration du système d'exploitation, incluant les données sur les logiciels installés.

Bref, on peut voir la base de registre comme le cerveau d'un ordinateur. On y trouve la configuration de Windows et les paramètres des logiciels installés, inscrits sous forme de clés. Il est important de savoir que ces clés sont rédigées dans un langage **complexe**, raison pour laquelle **on doit posséder les connaissances nécessaires lorsqu'on y apporte des changements**.

Il existe toutefois des logiciels spécialement conçus pour aider les individus à manipuler la base de registre à des fins précises. Par exemple, le logiciel CCleaner permet de « faire le ménage » dans la base de registre.

Anglais : *Registry*

Sources : Grand dictionnaire terminologique, Le Jargon français.

BIOS : Programme d'instruction présent dans tous les ordinateurs de type PC. Le BIOS accomplit deux types de tâches :

1. Au démarrage de l'ordinateur, il s'assure que le système d'exploitation est bien adapté aux composantes matérielles (disque dur, barrettes de mémoire, écran, etc.). Bref, il vérifier si tout est prêt et fonctionnel.
2. Il gère le transfert de l'information entre toutes les composantes d'un ordinateur, qu'elles soient matérielles ou logicielles. Bref, il agit comme un agent de liaison entre le matériel d'un ordinateur (le tangible) et ses logiciels (le non-tangible).

Acronyme de : *Basic Input/Output System*

Sources : Grand dictionnaire terminologique, MSN Encarta, Le Jargon français, Wikipédia, Wikipedia

Bit : Plus petite unité d'information avec laquelle peut travailler un ordinateur. Il ne peut prendre que les valeurs 0 ou 1, raison pour laquelle le bit fait partie de ce qu'on appelle le « langage binaire ».

CULTURE GÉNÉRALE

Il ne faut pas confondre le bit avec le *byte*, qui est le terme anglophone utilisé pour « octet ».

Anglais : *Bit*

Sources : Grand dictionnaire terminologique, Le Jargon français

Bombe logique : Petit programme lié à un logiciel malveillant. Il permet d'en programmer le déclenchement à une date précise ou à la suite d'une action (ou d'une série d'actions) particulière.

Exemple : Le virus Tchernobyl contenait une bombe logique qui en paramétrait le déclenchement pour le 26 avril, date anniversaire de la tristement célèbre explosion.

Anglais : *Logic Bomb*

Sources : Grand dictionnaire terminologique, Le Jargon français, Wikipedia.

Bot informatique : Petit logiciel (ou agent logiciel) utilisé pour automatiser des tâches répétitives, comme le ferait un robot.

Plusieurs bots sont conformes et légitimes. Par exemple, les wikis les

utilisent pour exécuter des tâches récurrentes comme la correction des fautes d'orthographe.

Cependant, d'autres bots peuvent être utilisés à des fins malicieuses. Par exemple, des bots « spammeurs » affichent de la publicité non sollicitée sur les forums et les blogues, ou encore recueillent des adresses courriel pour bâtir des listes de diffusion destinées au pourriel.

Anglais : *Internet Bot*

Sources : Wikipédia, Wikipedia.

Certificat électronique : Document numérique, émis par une autorité de certification, servant à lier une entité numérique (par exemple, un site Web) à une entité physique (par exemple, un serveur) afin d'assurer la fiabilité et la sécurité de l'entité numérique.

Synonyme : Certificat numérique
Anglais : *Digital certificate*

Sources : Grand dictionnaire terminologique, Wikipédia, Le Jargon français

Charge finale : Dans un virus, il s'agit de la portion de code exécutable dictant l'action malveillante à poser (par exemple, le formatage d'un disque dur, la suppression de certains fichiers, etc.).

Le virus contient deux composantes : la charge finale et le dispositif de reproduction (ce qui lui permet de se propager).

Anglais : *Payload*

Sources : Grand dictionnaire terminologique, Le Jargon français

Ciblage comportemental : Technique visant à augmenter l'efficacité d'une campagne publicitaire sur Internet. Elle permet d'afficher, sur l'ordinateur d'un internaute, de la publicité personnalisée selon ses besoins, ses intérêts et ses habitudes.

Le ciblage comportemental peut être une bonne tactique publicitaire si l'attention et le soin qu'il requiert lui sont apportés. Avec l'encadrement requis, cette technique est intéressante, mais elle peut rapidement causer des dérapages entre de mauvaises mains, ou simplement entre des mains malhabiles. La protection de la vie privée des internautes peut alors être compromise.

Anglais : *Behavioral Targeting*

Sources : Wikipédia, Wikipedia

Clavardage : Activité en ligne où un internaute converse avec d'autres internautes en échangeant des messages tapés au clavier.

Contrairement à un forum, où les échanges sont en temps différé (délai entre les messages), le clavardage permet une discussion en temps réel (aucun délai entre les messages).

Synonyme : Cyberbavardage
Variante : Tchate
Anglais : *Chat*

Sources : Grand dictionnaire terminologique, Wikipedia, Le Jargon français.

Clé de registre : Dans le système d'exploitation Windows, il s'agit d'une ligne de données inscrite dans la base de registre. Elle contient des valeurs qui font référence à un paramètre du système d'exploitation ou à un logiciel installé.

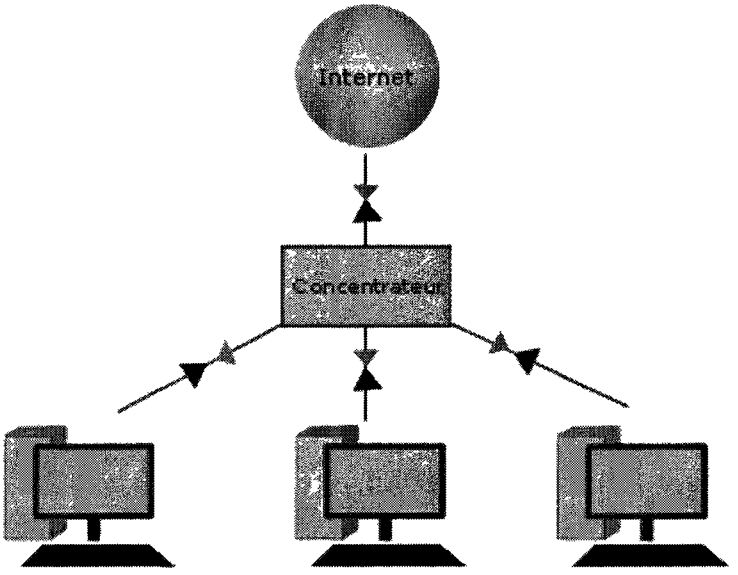
Exemple de rédaction d'une clé de registre :
HKEY_LOCAL_MACHINE\Logiciel\Concepteur\Nom de l'application\Version\Configuration

Anglais : *Registry Key*

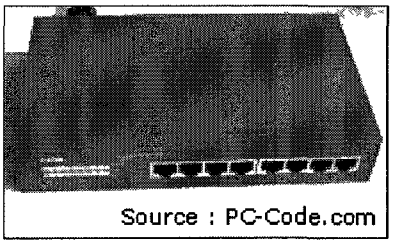
Source : Wikipedia

Concentrateur : Semblable à un routeur, le concentrateur est un appareil qui a pour objectif de diviser une « grosse » transmission de données en plusieurs « petites » transmissions, et vice versa.

Prenons l'exemple de plusieurs ordinateurs, dans un seul domicile, connectés à Internet. Le concentrateur peut diviser la « grosse » connexion en plus « petites » connexions afin de permettre aux ordinateurs d'avoir accès à Internet et d'être accessibles à partir d'Internet.



Le routeur et le concentrateur peuvent paraître similaires. Pourtant, à l'inverse de son proche cousin, le concentrateur n'héberge pas de logiciel et par conséquent, ses capacités se limitent à la division et au regroupement d'une transmission de données.


Source : PC-Code.com

Anglais : *Hub*

Sources : Grand dictionnaire terminologique, Le Jargon français

Conditions d'utilisation : Dans le contexte du Web, il s'agit de dispositions légales énoncées par un concepteur (d'un logiciel ou d'un site Web) concernant l'utilisation de son produit. Ces dispositions ont pour objectif de protéger légalement à la fois le concepteur et les utilisateurs.

Anglais : *Terms and Conditions of Use*

Source : Grand dictionnaire terminologique

Copier-coller : Le copier-coller permet de faire une copie d'un élément (texte, image, etc.) et de la coller ailleurs.

CULTURE GÉNÉRALE

Pour **copier**, sélectionnez l'élément à copier et cliquez dessus avec le bouton droit de la souris. Sélectionnez ensuite le menu Copier. Ou encore, appuyez simultanément sur les touches CTRL et C (la lettre C).

Pour **coller**, allez à l'endroit où vous voulez placer la copie, cliquez avec le bouton droit de la souris et sélectionnez le menu Coller, ou encore appuyez simultanément sur les touches CTRL et V (la lettre V).

Anglais : *Copy and paste*

CPU : Partie d'un ordinateur (constituée du ou des processeurs, en plus de la mémoire) où toutes les données de tous les programmes programmes sont traitées.

CULTURE GÉNÉRALE

Pour voir l'activité de votre CPU sous Windows, appuyez simultanément sur les touches CTRL, ALT et Supprime (Delete). Cliquez ensuite sur l'onglet Performance.

Français : Unité centrale
Acronyme de : *Central Processing Unit*

Source : Grand dictionnaire terminologique, Wikipédia

Cybercriminalité : Acte criminel commis avec de l'équipement informatique habituellement connecté à Internet.

Synonyme : Cyberdélinquance
Anglais : *Cyber criminality*

Source : Grand dictionnaire terminologique, Wikipédia

Page suivante ››

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la securite Internet
Maîtrise en etudes françaises, cheminement comunication et langages
Universite de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

GLOSSAIRE

Disque dur : Dispositif de stockage où sont enregistrées, de manière permanente, toutes les données d'un ordinateur (fichiers, logiciels et surtout, le système d'exploitation).

> **CULTURE GÉNÉRALE**
>
> Les disques durs d'aujourd'hui peuvent contenir une quantité impressionnante de données, jusqu'à 500 Go pour un ordinateur portable et 1 To (téraoctets, ou mille milliards d'octets) pour un ordinateur de bureau En avril 2009, la plus importante capacité enregistrée était de plus de 2 To

Synonyme : Disque rigide
Anglais : *Hard drive*

Sources : Grand dictionnaire terminologique, Le Petit Robert, Wikipédia, Wikipedia.

DNS : Système permettant d'établir un lien entre une adresse IP et un nom de domaine afin de diriger un internaute vers un site Web. Un nom de domaine, rédigé en lettres, est plus accessible pour les internautes que les chiffres de l'adresse IP.

On peut comparer le DNS à un bottin téléphonique : dans les deux cas, on parle d'un système qui fait le lien entre une entité chiffrée et une série de lettres.

Par exemple, l'adresse IP « 132.210.0.1 » (les deux derniers segments étant variables) fait référence au nom de domaine « usherbrooke.ca ».

Pour en savoir plus, consultez la fiche Fonctionnement du DNS.

Acronyme de : *Domain Name System*

Sources : Le Jargon français, Wikipédia.

Droits administrateurs : L'administrateur d'un système est l'utilisateur qui a tous les droits. Il peut par conséquent effectuer presque toutes les manipulations possibles.

Les droits administrateurs sont ceux qui sont exclusifs à l'administrateur et que les autres utilisateurs ne possèdent pas.

Anglais : *Admin rights*

Source : Le Jargon français

Ergonomie Web : Discipline connexe de l'ergonomie visant à adapter ou à créer « des contenus et des fonctionnalités d'un site Web en vue d'en faciliter l'utilisation par ses visiteurs » (Grand dictionnaire terminologique). L'ergonomie Web regroupe deux composantes, l'utilité et l'utilisabilité.

Source : Grand dictionnaire terminologique

Extension de nom de fichier : Série de trois ou quatre caractères précédée d'un point et placée après le nom d'un fichier. L'extension sert à reconnaître le format du fichier et à activer le logiciel approprié lorsque le fichier est sollicité.

Exemples : mon_joli_document**.doc** (fichier Word); une_page_Web**.html**; suis-je_fiable**.exe**

Notes :

- Les fichiers munis d'une extension « .exe » sont à potentiellement risqués, puisqu'ils exécutent des scripts. Par exemple, certains virus informatiques prennent la forme d'un fichier doté d'une extension « .exe ».
- Les fichiers « .zip », « .rar », « .cmd », « .bat », « .pif », « .com » et « .scr » sont également à manipuler avec précaution.

Synonyme : Extension
Anglais : *Filename extension*

Sources : Grand dictionnaire terminologique, Wikipédia

Faiblesse humaine : Dans un contexte informatique, il s'agit d'un défaut dont l'utilisateur est responsable et qui le rend vulnérable à une attaque. Une faiblesse humaine apparaît lorsqu'un utilisateur ne prend pas les dispositions technologiques nécessaires pour assurer sa sécurité, ou qu'il les entreprend de la mauvaise manière.

La faiblesse humaine peut donc être un logiciel de sécurité manquant ou qui n'est pas à jour, ou encore une faible protection lors des transferts de données.

Il ne faut pas confondre les faiblesses humaines avec les failles de sécurité, qui sont issues de défauts dans la programmation du code d'un logiciel.

Faille de Défaut dans un logiciel permettant une manipulation imprévue, comme

sécurité : l'infiltration d'un logiciel malveillant.

Les failles de sécurité sont habituellement des erreurs dans la programmation d'une application. L'utilisateur n'est pas lié à leur apparition. Toutefois, il doit se protéger en installant les correctifs de sécurité offerts par les fournisseurs des logiciels. Ces correctifs se trouvent presque toujours dans les mises à jour.

> **CULTURE GÉNÉRALE**
>
> Aucun logiciel n'est exempt de failles et les fournisseurs de logiciel publient régulièrement des correctifs de sécurité à télécharger.

Il ne faut pas confondre les failles de sécurité avec les faiblesses humaines, qui sont issues d'un manque ou d'une mauvaise manipulation de l'utilisateur.

Synonyme : Vulnérabilité
Anglais : *Vunerability*

Sources : Grand dictionnaire terminologique, Le Jargon français.

Favori : Hyperlien vers une page Web mis en mémoire par un internaute pour faciliter son repérage ultérieur.

Synonymes : Marque-page, signet
Anglais : *Favorite*

Sources : Grand dictionnaire terminologique, Le Jargon français

Fenêtre pop-up : Fenêtre secondaire non sollicitée qui s'affiche devant la fenêtre du navigateur et qui peut présenter de la publicité.

Synonymes : Fenêtre intempestive, fenêtre intruse
Anglais : *Pop-up ad, pop-up window*

Sources : Grand dictionnaire terminologique, Wikipédia

Feuille de style (CSS) : Feuilles de style dites en cascade permettant de gérer la présentation (ou l'apparence) entre autres des documents HTML.

CSS est un acronyme de : *Cascading Style Sheet*

Sources : Grand dictionnaire terminologique, Wikipedia.

Fil d'Ariane : Suite de titres, « chacun représentant une subdivision de la carte du site, qui donne à l'internaute un aperçu du chemin parcouru et lui permet de repérer facilement sa position dans l'arborescence du site Web visité » (Grand dictionnaire terminologique).

Sources : Grand dictionnaire terminologique

Formatage : Action de préparer un support (comme un disque dur ou une disquette) pour qu'il soit en mesure d'accueillir de l'information dans un format précis.

Lorsqu'on parle du formatage d'un disque dur, cela signifie que l'espace disque est formaté pour accueillir de la nouvelle information. Bref, le contenu du disque dur sera supprimé afin de préparer l'espace pour de nouvelles données.

Anglais : *Format*

Sources : Grand dictionnaire terminologique, Le Jargon français, Wikipédia.

Forum : Espace virtuel, souvent une page Web, où plusieurs internautes discutent de sujets en tous genres. Les échanges se font en temps différé (délai entre les messages), contrairement au clavardage où les échanges sont en temps réel (aucun délai entre les messages).

CULTURE GÉNÉRALE

Il n'y a pas que les sites Web qui offrent des forums de discussion; les groupes de *news* et les blogues sont d'autres lieux où peuvent se tenir des échanges asynchrones (en temps différé).

Exemple de forum informatique : Commentçamarche.net

Synonymes : Forum de discussion, groupe de discussion
Anglais : *Forum*

Sources : Grand dictionnaire terminologique, Wikipédia.

Fournisseur d'accès à Internet : Entreprise mettant à la disposition des individus et des entreprises un accès au réseau Internet moyennant certains frais.

Exemples de FAI : Bell Internet (anciennement Sympatico), Vidéotron, Radioactif, etc.

Abréviation : FAI
Anglais : *Internet Service Provider*

Sources : Grand dictionnaire terminologique, Le Jargon français.

Fraude psychologique (ingénierie sociale) : Ensemble de moyens utilisés par un fraudeur pour tromper et manipuler un individu. L'objectif est de l'inciter à commettre des actions ou à remettre de l'information confidentielle pour permettre au fraudeur de s'introduire illégalement dans un système, qu'il s'agisse du réseau d'une entreprise, du compte de banque d'un individu ou de tout autre système.

Anglais : *Social engineering*
Autre terme (non retenu) : Ingénierie sociale

Sources : Grand dictionnaire terminologique, Le Jargon français

FTP : Protocole permettant le transfert de fichiers d'un ordinateur client vers un serveur et vice versa.

Acronyme de : *File Transfer Protocol*

Source : Grand dictionnaire terminologique

Gel : Situation où un logiciel s'interrompt de manière soudaine et inattendue. Contrairement à un plantage, lors d'un gel, l'ordinateur est toujours en mesure de répondre à quelques commandes.

Dans certains cas, le gel se résorbe de lui-même. Dans d'autres cas, il est possible de fermer l'application gelée en appuyant simultanément sur les touches CTRL, ALT et Supprime (Delete), puis en mettant un terme à l'application gelée. Certains gels sérieux peuvent toutefois nécessiter le redémarrage de l'ordinateur.

Anglais : *Freeze*

Sources : Le Jargon français, Wikipedia.

Gratuiciel : Logiciel pouvant être téléchargé et utilisé gratuitement. Il peut être copié et distribué sans frais. Le concepteur du gratuiciel conserve toutefois son code source et ses droits d'auteur.

Exemple : Le logiciel antiespiogiciel SpyBot Search & Destroy

À ne pas confondre avec le partagiciel ni avec le logiciel libre et gratuit.

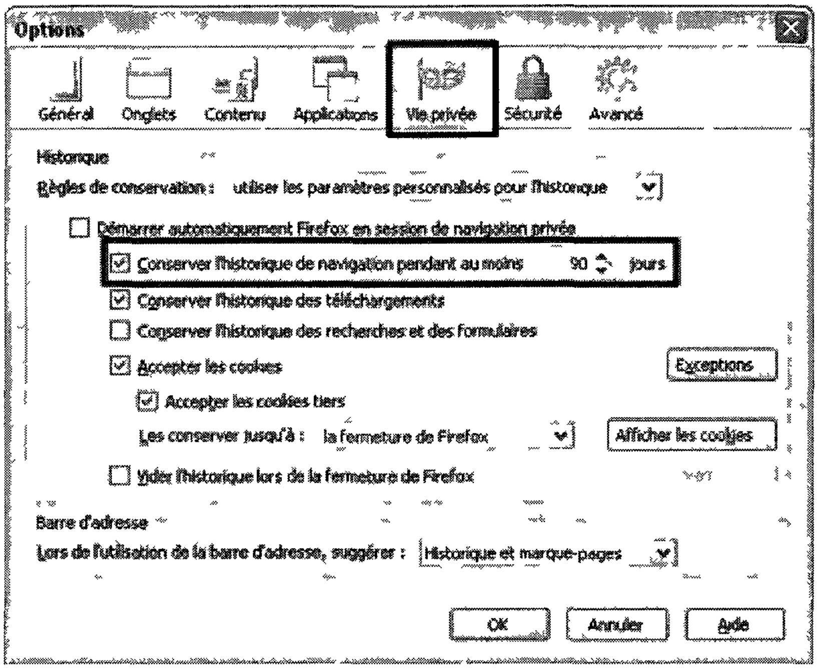
Anglais : *Freeware*

Sources : Grand dictionnaire terminologique, Wikipedia, Wikipédia

Historique de navigation : Fichier où sont sauvegardées toutes les adresses des pages Web visitées dans une période donnée (hebdomadairement, au cours du mois, etc.).

L'historique est accessible par le navigateur. L'utilisateur peut lui-même définir la durée de conservation des données dans l'historique.

Dans le navigateur Mozilla Firefox, ce paramètre peut être modifié dans le menu Outils/Options/[Onglet] Vie privée :



Anglais : *Browsing History*

Source : Wikipédia

HTML : Langage de balisage hypertexte qui permet la création de pages Web pouvant être visionnées à l'aide d'un navigateur.

Acronyme de : *Hypertext Markup Language*

Sources : Grand dictionnaire terminologique, Wikipédia

IMAP : Protocole de messagerie électronique permettant la réception (et plus précisément, la consultation) des courriels.

Acronyme de : *Internet Message Access Protocol*

Source : Grand dictionnaire terminologique

Infobulle : « Élément d'un système d'aide contextuelle qui, à la demande de l'utilisateur, affiche de l'information » (Grand dictionnaire terminologique) complémentaire.

Sources : Grand dictionnaire terminologique, Wikipédia

IP : Protocole qui donne à chaque ordinateur (client ou serveur) une adresse unique (adresse IP) pour rendre les échanges possibles.

Acronyme de : *Internet Protocol*

Internet : Réseau informatique mondial reliant des ordinateurs qui peuvent communiquer entre eux grâce au protocole TCP/IP.

Sources : Grand dictionnaire terminologique, Le Jargon français, Wikipedia, Wikipédia

Sources : Grand dictionnaire terminologique, Le Jargon français, Wikipedia, Wikipédia

JavaScript : Langage de script, développé par Netscape et simplifié pour les utilisateurs débutants, servant à apporter du dynamisme aux pages Web.

Sources : Grand dictionnaire terminologique, Le Jargon français, Wikipedia, Wikipédia

Licence d'utilisation d'un logiciel : Contrat entre un concepteur et un utilisateur où le concepteur (détenteur des droits d'auteur) autorise l'utilisateur à employer le logiciel. Cette licence comporte des conditions, dont les conditions d'utilisation.

Il revient à l'utilisateur d'accepter ou non la licence; s'il ne s'y conforme pas, il ne pourra pas utiliser le logiciel.

Anglais : *Software license*

Sources : Grand dictionnaire terminologique, Wikipédia

Logiciel « de ménage » : Petit logiciel qui permet d'optimiser le fonctionnement d'un ordinateur et la protection de la vie privée de l'internaute.

Il « fait le ménage » dans l'ordinateur et dans la base de registre pour supprimer toutes les traces laissées par l'internaute lors de sa navigation (fichiers inutiles pouvant contenir des renseignements confidentiels, historique, etc.) et les traces laissées par certains logiciels malveillants (clés de registre inutiles ou malveillantes, etc.).

Logiciels « de ménage » gratuits :

- CCleaner (anglais);
- Advanced SystemCare (en anglais uniquement).

Source : Wikipédia

Logiciel antiespiogiciel : Logiciel de sécurité visant à détecter et, si possible, à éliminer les espiogiciels et, dans certains cas, les logiciels publicitaires, les témoins traceurs et les chevaux de Troie.

Logiciels antiespiogiciels gratuits :

- Spybot Search & Destroy;
- Ad-Aware;
- Emisoft Anti-Malware;
- Windows Defender (anglais);
  Attention, ce logiciel est intégré aux systèmes d'exploitation

Windows Vista et Windows 7. Il n'est pas fourni avec Windows XP.
- Malwarebytes Antimalware.

IMPORTANT

Pensez à installer au moins deux logiciels antiespiogiciels et à scanner votre ordinateur avec chaque antiespiogiciel au moins une fois par semaine.

QUESTION

« Pourquoi installer deux logiciels antiespiogiciels, un seul n'est-il pas suffisant? » La réponse pourrait se résumer en une phase : un antiespiogiciel c'est bien, mais deux c'est mieux.

L'objectif du logiciel antiespiogiciel est d'éradiquer les espiogiciels, qui eux permettent de recueillir des données servant à... envoyer de la publicité. C'est un domaine très rentable et plusieurs entreprises n'hésiteront pas à tenter de soudoyer (avec ou sans succès) les concepteurs d'antiespiogiciels pour que leurs mouchards échappent au radar.

Avec deux logiciels antiespiogiciels, on augmente donc les chances d'éradication : ce que l'un omettra de trouver pourra être découvert par l'autre.

Synonyme : Logiciel anti-logiciel espion
Anglais : *Antispyware software*

Sources : Grand dictionnaire terminologique, Wikipédia, Wikipedia.

Logiciel *antirootkit* : Logiciel de sécurité visant à détecter et, si possible, à éliminer les *rootkits*.

IMPORTANT

Ces logiciels spécialisés s'acquittent assez bien de leur tâche, dans l'ensemble. C'est au niveau de l'utilisation qu'ils diffèrent : certains sont simples à utiliser, d'autres non. Il est important de choisir le bon logiciel en fonction de son niveau d'aisance informatique.

Logiciels *antirootkit* gratuits :

- Sophos Anti-Rootkit, simple à manipuler;
- Rootkit Revealer (anglais), plus complexe.

ATTENTION

Une fois l'analyse *antirootkit* terminée, observez bien les résultats... Si vous avez créé un fichier qui nécessite un mot de passe à l'ouverture (par exemple, un fichier de compression WinRar), il se peut qu'il soit perçu comme un *rootkit*. Vous savez toutefois qu'il n'en est pas un. Utilisez votre jugement et faites attention à ce que vous supprimez.

N'hésitez pas à créer un point de restauration avant de procéder à une suppression, au cas où Windows deviendrait dysfonctionnel par la suite. Si cela survient, vous pourrez alors ramener votre ordinateur à l'état où il était avant la suppression du ou des fichiers.

Anglais : *Antirootkit software*

Sources : Grand dictionnaire terminologique, Wikipédia, Wikipedia.

Logiciel antivirus :

Logiciel de sécurité visant à détecter l'intrusion de certains parasites (dont les virus, les vers informatiques et les chevaux de Troie), à les neutraliser et si possible, à les éliminer.

Certains logiciels antivirus sont accompagnés d'un antiespiogiciel, d'un *antirootkit*, d'un pare-feu, d'un filtre de pourriel, etc. Dans ces cas, on parle davantage d'une suite de logiciels de sécurité (*Internet Security*).

De nos jours, les simples logiciels antivirus sont de plus en plus rares; ils sont désormais accompagnés d'autres logiciels de sécurité, et ce, même s'ils conservent l'appellation « antivirus ».

À cet effet, chaque mention « logiciel antivirus » dans ce site fait également référence aux suites de logiciels de sécurité.

Logiciels antivirus gratuits :

- Avast;
- Antivir.
- Le site AV-Comparatives.org teste annuellement les logiciels antivirus (majoritairement payants) disponibles sur le marché. Consultez leurs rapports annuels pour vous aider dans votre recherche de logiciel.
    - Rapports annuels d'AV-Comparatives.org (anglais)

Conseils :

- Activez votre logiciel antivirus en tout temps.
- Maintenez régulièrement les signatures d'infection à jour.
- Pensez à scanner votre ordinateur avec votre antivirus au moins deux fois par mois.
- « Magasinez » bien votre antivirus. Comme mentionné ci-haut, chaque logiciel ou suite de logiciels offre des solutions différentes. Renseignez-vous avant de choisir et optez ensuite pour celui qui répond à vos besoins et vos critères. Si vous avez besoin d'un coup de main, consultez les Questions et réponses.

Anglais : *Antivirus software*

Sources : Grand dictionnaire terminologique, Le Jargon français, Le Petit Robert, Wikipédia.

Logiciel de courriel :

Logiciel qui permet à un internaute de recevoir, de lire, de composer et d'envoyer des courriels. Il facilite également la gestion d'un ou de plusieurs comptes courriel.

La plupart des logiciels de courriel comprennent un filtre antipourriel pour protéger l'internaute contre les pourriels, les courriels d'hameçonnage et les autres courriels indésirables ou frauduleux.

Logiciels de courriel gratuits :

- Mozilla Thunderbird;
- Eudora (anglais).

Synonyme : Client de messagerie, logiciel de messagerie, courrielleur
Anglais : *E-mail software*

Source : Wikipédia, Grand dictionnaire terminologique

Logiciel de désinstallation :

Logiciel conçu pour aider l'utilisateur d'un ordinateur à supprimer un logiciel et ses diverses traces.

En plus d'effectuer la désinstallation, il est en mesure de faire certaines analyses visant à détecter et à supprimer toutes les traces laissées par le logiciel désinstallé (fichiers et clés de registre inutiles).

Logiciel gratuit :

- Revo Uninstaller (anglais)

ATTENTION

Ce type de logiciel manipule parfois la base de registre lorsque certaines clés problématiques doivent être supprimées. Portez une attention particulière à cette étape.

Si vous remarquez que le système d'exploitation Windows agit bizarrement après une désinstallation, c'est peut-être parce qu'une clé essentielle a été supprimée. Vous pouvez alors utiliser la restauration de système pour tenter de corriger la situation.

Anglais : *Uninstalling software*

Source : Assiste.com

Logiciel de gestion des mots de passe :

Logiciel permettant de gérer plusieurs mots de passe et noms d'utilisateurs. Il regroupe l'ensemble des mots de passe et des identifiants employés par un usager et les stocke dans une base de données sécurisée, accessible par un mot de passe unique. Ainsi, l'utilisateur n'a qu'un mot de passe à retenir.

En plus, ce logiciel chiffre les mots de passe enregistrés, ce qui empêche tout individu (autre que le propriétaire) d'avoir accès à ces précieux

renseignements.

Logiciel gratuit :

- KeePass Password Safe (anglais)

Anglais : *Password manager software*

Sources : KeePass.info, Wikipédia.

Logiciel de pair-à-pair :

Logiciel permettant l'échange de fichiers par Internet (musique, films, images, logiciels, etc.).

La particularité des logiciels de pair-à-pair est qu'ils permettent à deux ordinateurs de se connecter entre eux sans passer par un serveur central. C'est bien pratique pour avoir accès à tous les fichiers désirés, mais problématique au point de vue de la sécurité. Et si les fichiers téléchargés étaient infectés, factices ou corrompus? Et si l'ordinateur auquel on se connectait était infecté ou malveillant?

ATTENTION

Les logiciels de pair-à-pair peuvent être bien tentant par la quantité de fichiers auxquels ils donnent accès. Toutefois, leur utilisation est potentiellement illégale (car plusieurs fichiers sont illégaux) et surtout, très risquée.

Exemples : KaZaA, LimeWire, eMule, BitTorrent, etc.

Synonyme : Poste-à-poste
Abréviation : P2P
Anglais : *Peer-to-peer*

Sources : Grand dictionnaire terminologique, Wikipédia.

Logiciel de rechange :

De nos jours, les logiciels utilisés massivement (peu importe leur type : traitement de texte, lecteur de musique, navigateur, etc.) sont une cible de choix pour les pirates. Dans une attaque de grande envergure, les logiciels malveillants doivent pouvoir infiltrer le plus d'ordinateurs possible. Ils cibleront alors un logiciel populaire, installé sur la majorité des ordinateurs, et l'utiliseront comme porte d'entrée en exploitant l'une de ses failles.

En possédant des logiciels moins connus, souvent gratuits et en plus, très efficaces, un internaute réduit le risque d'attaque.

Assiste.com a mis sur pied une « logithèque alternative » contenant des logiciels de rechange gratuits et surtout, propres (sans espiogiciels ni autres logiciels malveillants).

- Logithèque alternative d'Assiste.com

Il existe quelques incontournables, énumérés ci-dessous. Pour tous les autres, il y a la logithèque alternative d'Assiste.com.

- Mozilla Firefox, Google Chrome ou Opera, pour remplacer Internet Explorer;
- Mozilla Thunderbird ou Eudora (anglais), pour remplacer Outlook;
- aMSN (anglais), Pidgin (anglais) ou Trillian (anglais), pour remplacer MSN Messenger/Windows Live Messenger;
- Foxit Reader (anglais), pour remplacer Adobe Reader;
- Winamp ou Songbird (anglais), pour remplacer Windows Media Player;
- Et encore plus.

Source : Assiste.com

Logiciel libre et gratuit :

Logiciel gratuit dont la licence est libre d'utilisation et donc, sans frais. Ce type de logiciel est habituellement développé dans un contexte de « logiciel libre », où plusieurs programmeurs s'échangent le code source afin de le perfectionner.

Exemples : La suite bureautique OpenOffice, le système d'exploitation Linux

À ne pas confondre avec le gratuiciel ni avec le partagiciel.

Anglais : *Free Software*

Sources : Grand dictionnaire terminologique, Wikipédia, Wikipedia

‹‹ Page précédente ... Page suivante ››

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

GLOSSAIRE

Mémoire cache : Dans le contexte du Web, lorsqu'un site est visité, la mémoire cache stocke certains fichiers (comme les images) afin d'accélérer le chargement du site lors d'une visite ultérieure. Ces fichiers sont aussi appelés des fichiers temporaires.

Hors Web, il s'agit d'une mémoire petite tampon très rapide qui permet d'accélérer les traitements lors de certaines activités informatiques.

Synonyme : Cache
Anglais : *Cache memory*

Sources : Wikipédia, Grand dictionnaire terminologique

Mémoire vive : Mémoire rapide d'un ordinateur. Elle n'est pas permanente, puisqu'elle s'efface dès que l'ordinateur est mis hors tension, mais elle est essentielle au fonctionnement des logiciels.

Si un ordinateur ne possède pas assez de mémoire vive, son fonctionnement peut être ralenti, voire impossible, lors de l'exécution de plusieurs logiciels en simultanée, ou encore de certains logiciels gourmands (par exemple, un logiciel de traitement de l'image ou un logiciel de montage vidéo).

Synonyme : RAM
Anglais : *Random Access Memory*

Sources : Grand dictionnaire terminologique, Le Jargon français

Messagerie instantanée : Service de clavardage en temps réel. Grâce à un logiciel, l'utilisateur a accès à une liste personnalisée de contacts en ligne avec qui il peut immédiatement entrer en communication.

Exemples de logiciels de messagerie instantanée : Windows Live Messenger / MSN Messenger, Yahoo! Messenger, ICQ.

Logiciels de messagerie instantanée alternatifs :

- aMSN (anglais);
- Pidgin (anglais);
- Trillian (anglais).

Anglais : *Instant messaging*

Sources : Grand dictionnaire terminologique, Le Jargon français

Mode sans échec : Mode d'exécution permettant de démarrer un ordinateur avec le minimum de ressources logicielles, c'est-à-dire uniquement avec le système d'exploitation et certains pilotes (les logiciels nécessaires au fonctionnement des périphériques). Majoritairement utilisé en cas de problèmes, ce mode permet de détecter les incidents sans que l'ordinateur ne soit « brouillé » par des logiciels non essentiels à son fonctionnement ni par des logiciels malveillants.

Pour savoir comment démarrer un ordinateur en mode sans échec, consultez la fiche Mode sans échec.

Anglais : *Safe Mode*

Sources : Grand dictionnaire terminologique, Wikipedia

Moteur de recherche : Sur le Web, il s'agit d'un programme (présenté dans une page Web) couplé à une base de données indexant de nombreux sites Web. Lors de ses recherches Web, l'internaute peut accéder à ces sites en utilisant des mots-clés.

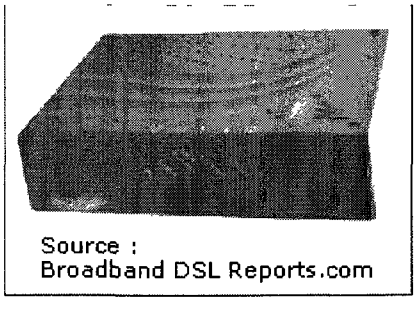
Exemples : Google, Yahoo!, Bing, etc.

Anglais : *Search Engine*

Sources : Grand dictionnaire terminologique

Modem : Appareil qui permet à un ordinateur (ou à un réseau) de se connecter à Internet.

Il a pour principale fonction de transformer un signal analogique (issu du câble ou de la ligne téléphonique) en signal numérique, car il ne faut pas oublier que les ordinateurs ne parlent que le numérique.



Sources : Grand dictionnaire terminologique, Le Jargon français

Navigateur : Logiciel permettant la consultation et l'exploration du *World Wide Web*. Il prend en charge la consultation de moteurs de recherche,

d'applications Web, de sites Web, etc., tout en permettant à l'internaute d'interagir avec les contenus (texte, audio, vidéo, etc.).

CULTURE GÉNÉRALE

De nos jours, les navigateurs ne sont plus exclusifs aux ordinateurs, on les trouve également sur d'autres dispositifs technologiques pouvant être connectés à Internet comme les consoles de jeu vidéo, les téléphones intelligents, les assistants numériques personnels (ANP), etc.

Comme plusieurs autres logiciels, le navigateur peut contenir des brèches, parfois petites, parfois grandes. Pour qu'elles soient « colmatées », il doit être régulièrement mis à jour.

Certains navigateurs offrent des mises à jour automatiques et d'autres affichent des avis lorsqu'une mise à jour doit être installée. Si tel est le cas, il est important de ne pas ignorer ces messages et de procéder aux installations.

Navigateurs gratuits :

- Mozilla Firefox;
- Google Chrome;
- Opera.

IMPORTANT

Les navigateurs d'aujourd'hui offrent différentes protections, dont le repérage des sites factices ou frauduleux (pouvant entre autres être liés à des courriels d'hameçonnage). Cette dernière protection est habituellement activée par défaut et pour une sécurité optimale, l'internaute est invité à ne pas la désactiver.

Synonymes : Fureteur, explorateur.
Anglais : *Browser*

Sources : Grand dictionnaire terminologique, Wikipédia.

Nom de domaine :

Équivalence alphabétique d'une adresse IP. Il s'agit d'une série de caractères identifiant le nom d'un site Web et son domaine (.com, .ca, .fr, etc.) dans une adresse URL.

Une adresse URL respecte le modèle suivant : http://www.exemple.com. Dans ce modèle, la mention « http:// » fait référence au protocole utilisé et « exemple.com » est le nom de domaine.

CULTURE GÉNÉRALE

Le nom de domaine est un identifiant unique sur le Web; aucun nom de domaine n'existe en double.

Anglais : *Domain name*

Sources : Grand dictionnaire terminologique, Wikipédia.

Octet : Unité de mesure informatique évaluant la taille des données. Chaque octet contient huit bits.

On parle plus souvent de kilooctets (Ko), de mégaoctets (Mo) et de gigaoctets (Go).

Exemples : un fichier Word de 42 Ko, une photographie de 2,8 Mo et un disque dur de 320 Go.

Anglais : *Byte*

Sources : Grand dictionnaire terminologique, Wikipédia, Le Jargon français

Ordinateur client : Dans une approche client-serveur, l'ordinateur client est un ordinateur « normal », celui possédé par un individu et utilisé pour demander de l'information par la formulation de requêtes auprès d'un serveur.

Approche client-serveur :
On peut comparer le serveur à un gros « centre de distribution » et le client, à une petite « usine de traitement ». Lorsque le serveur reçoit une requête d'un ordinateur client, il lui envoie (ou « distribue ») les données nécessaires pour répondre à cette requête. Par la suite, l'ordinateur client traite ces données pour que l'utilisateur puisse en profiter.

Synonyme : Client
Anglais : *Client*

Source : Grand dictionnaire terminologique, Le Jargon français

Ordinateur zombie : Ordinateur infecté et rallié de force à un *botnet*, où il est contrôlé par un pirate. Le pirate utilise la bande passante (ou la puissance de la connexion Internet) de l'ordinateur infecté, combinée à celle des autres ordinateurs zombies du *botnet*, pour commettre des actes de grande envergure comme un envoi massif de pourriels ou une attaque par refus de service.

Anglais : *Zombie computer*

Source : Grand dictionnaire terminologique

Parasite : Logiciel non sollicité qui cause divers dommages logiciels et parfois matériels.

Anglais : *Parasite*
Synonyme: Logiciel malveillant

Source : Grand dictionnaire terminologique

Pare-feu : Dispositif de sécurité permettant de protéger un ordinateur (ou un réseau) connecté à Internet en filtrant les données qui entrent et qui sortent de l'ordinateur.

Il agit comme une sorte de « barrière coulissante » pour bloquer les tentatives d'intrusions en provenance d'Internet tout en laissant passer les données fiables, et comme une sorte de « douanier » pour contrôler les données qui sont envoyées vers Internet.

Il existe deux types de pare-feu : le matériel et le logiciel.

Le pare-feu **matériel** se situe habituellement à l'extérieur de l'ordinateur (par exemple, un routeur) et le pare-feu **logiciel** est un programme installé sur un ordinateur.

Dans le présent site Web, toutes les mentions « pare-feu » font référence au pare-feu logiciel.

Pare-feu gratuits :

- Outpost Firewall (anglais);
- Comodo Firewall (anglais) - Note : ce pare-feu fonctionne très bien sur les plateformes Windows 64-bits;
- Le site Matousec.com teste régulièrement les pare-feu disponibles sur le marché (gratuits et payants). Consultez-le pour choisir un pare-feu qui répondra à vos besoins et à vos critères.
    - Résultats des analyses de Matousec.com (anglais)

Conseils :

- Avant d'installer un pare-feu, vérifiez les fonctionnalités de votre logiciel antivirus, peut-être en offre-t-il déjà un. Il est important de n'installer qu'un seul pare-feu sur un ordinateur.
- Pour être efficace, un pare-feu doit être **bien paramétré**. Contrairement à ce qu'on pourrait croire, paramétrer un pare-feu n'a rien de sorcier. Lors de votre utilisation d'Internet, il fera apparaître des boîtes de dialogue qui se chargeront de ce paramétrage en vous demandant si vous autorisez (ou refusez) le transfert de données effectué par un logiciel ou un service. Votre décision sera alors enregistrée sous forme de règle et votre pare-feu la respectera à l'avenir.

Synonyme : Coupe-feu
Anglais : *Firewall*

Sources : Grand dictionnaire terminologique, Wikipédia, Le Jargon français, Softpedia (anglais), PC World (anglais)

Partagiciel : Logiciel pouvant être téléchargé et utilisé gratuitement pour une période ou un nombre d'utilisations déterminé, au terme de quoi l'utilisateur est fortement incité à l'acquérir.

Exemples : Le logiciel de compression WinZip, PDF 995 (logiciel de création de fichiers PDF).

À ne pas confondre avec le gratuiciel ni avec le logiciel libre et gratuit.

Anglais : *Shareware*

Sources : Grand dictionnaire terminologique, Wikipédia, Le Jargon français

PC : Ordinateur personnel utilisé par un individu à des fins personnelles ou liées au travail.

Acronyme de : *Personal Computer*

Sources : Grand dictionnaire terminologique, Wikipédia

Périphérique : Dispositif matériel connecté à un ordinateur et permettant l'entrée et (ou) la sortie de données.

Il existe trois types de périphériques :

1. entrée de données : clavier, souris, scanneur, manette de jeu, etc.;
2. sortie de données : écran, imprimante, haut-parleurs, etc.;
3. entrée-sortie de données : graveur DVD, clé USB, etc.

Pour que l'ordinateur soit en mesure de faire fonctionner certains périphériques, il a besoin d'un pilote, soit un logiciel servant d'intermédiaire entre l'ordinateur et le périphérique concerné.

Anglais : *Peripheral*

Sources : Grand dictionnaire terminologique, Wikipédia

PHP : Langage de script permettant la création de pages Web dynamiques pouvant être visionnées avec un navigateur.

Acronyme de : *Hypertext Preprocessor*

Sources : Grand dictionnaire terminologique, Le Jargon français.

Plantage : Situation où un logiciel s'interrompt de manière soudaine et inattendue.

Lors d'une telle panne, le logiciel en cause, et même tout l'ordinateur,

n'est plus en mesure d'exécuter les commandes de l'utilisateur et l'image à l'écran se fige. Le plantage nécessite habituellement un redémarrage de l'ordinateur.

Synonyme : Panne
Anglais : *Crash*

Sources : Grand dictionnaire terminologique, Le Jargon français.

Plugiciel : Élément logiciel complémentaire qui se greffe à un logiciel principal pour offrir une fonctionnalité supplémentaire. Une fois installé (ou mis à jour), le plugiciel interagit avec le logiciel principal sans que l'utilisateur n'ait à intervenir.

Exemple de plugiciel : Flash Player

Note : Dans le cadre de ce site, le « composant logiciel » et le « plugiciel » font référence au même élément logiciel complémentaire.

Synonymes : Module d'extension, greffon
Anglais : *Plug-in*

Sources : Grand dictionnaire terminologique, Wikipédia, Le Jargon français.

Polluposteur : Personne à l'origine des envois massifs de pourriels et de courriels d'hameçonnage.

Synonymes : Pourrielleur, inondeur.
Anglais : *Spammer*

Sources : Grand dictionnaire terminologique, Le Jargon français

POP3 : Protocole de messagerie électronique permettant la réception (et plus précisément, la récupération) des courriels.

Acronyme de : *Post Office Protocol Version 3*

Source : Grand dictionnaire terminologique

Port : Connexion virtuelle entre Internet et un ordinateur (client ou serveur) permettant la circulation des données.

On peut le comparer à une petite porte qui s'ouvre et se ferme au besoin. Lorsqu'il y a un certain contrôle de la circulation des données, on peut dire qu'un port est sécurisé.

Le pare-feu sert entre autres à surveiller certains ports à risque pour

empêcher l'infiltration d'un logiciel malveillant. Il permet également de sécuriser « manuellement » d'autres ports; n'hésitez pas à consulter les rubriques d'aide de votre pare-feu pour en savoir plus.

CULTURE GÉNÉRALE

Au total, 65 536 ports sont disponibles lorsqu'on se connecte à Internet. Certains sont plus utilisés que d'autres, comme le port 80 qui sert à la navigation sur le Web et le port 25 qui permet l'envoi de courriels.

Anglais : *Port*

Sources : Grand dictionnaire terminologique, Wikipedia.

Porte dérobée : Fonctionnalité cachée permettant d'ouvrir une brèche (« porte ») dans un logiciel pour qu'une tierce personne entre dans l'ordinateur à l'insu de l'utilisateur.

Certaines portes dérobées peuvent être légitimes et servir à des fins de maintenance ou de surveillance. Toutefois, d'autres portes dérobées sont secrètes et utilisées par des pirates pour entrer discrètement dans un système. Elles peuvent d'ailleurs être employées par les chevaux de Troie et les *rootkits*.

Synonyme : Trappe
Anglais : *Backdoor*

Sources : Grand dictionnaire terminologique, Le Jargon français, Wikipédia

Programme (ou logiciel) « hôte » : Logiciel auquel se greffe un virus informatique pour activer sa charge finale et se reproduire.

Exemples de programmes « hôtes » : un logiciel de traitement de texte, une composante logicielle du système d'exploitation, un petit jeu interactif téléchargé à partir d'Internet (dont l'extension est .EXE), etc.

Anglais : *Host program*

Source : Grand dictionnaire terminologique, Wikipédia

Protection antiespiogicielle en temps réel : Logiciel (ou fonctionnalité d'un logiciel) offrant une protection contre l'infiltration d'espiogiciels.

La protection antiespiogicielle en temps réel implique une activation constante du logiciel concerné, dès le démarrage de l'ordinateur. Il est alors en mesure d'empêcher, **au meilleur de ses capacités** (et de ses mises à jour), le téléchargement de logiciels malveillants, contrairement aux autres logiciels antiespiogiciels qui les éliminent uniquement à la suite d'une analyse.

Logiciels gratuits :

- SpywareBlaster (anglais);
- Windows Defender
  Attention, ce logiciel est intégré aux systèmes d'exploitation Windows Vista et Windows 7. Il n'est pas fourni avec Windows XP.

‹‹ Page précédente ... Page suivante ››

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise a jour 4 janvier 2011

Ce site a ete conçu dans le cadre d'un memoire production sur la securite Internet

Maîtrise en etudes françaises, cheminement comunication et langages

Universite de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

GLOSSAIRE

Quarantaine : Dans un contexte informatique, il s'agit d'une mise à l'écart, pour une période donnée, de certains fichiers infectés détectés par un logiciel de sécurité (antivirus, antiespiogiciel, etc.).

Sources : Wikipédia, Le Petit Robert

Refus de service : État d'un système, d'un serveur, d'un ordinateur ou d'un site Web où il n'est plus en mesure de fonctionner, puisqu'il ne peut plus répondre aux commandes des utilisateurs. Habituellement, le refus de service résulte d'une attaque ciblée.

Par exemple, un site Web peut planter (refus de service) à la suite d'une attaque par saturation.

Anglais : *Denial of service*

Sources : Grand dictionnaire terminologique, Wikipédia.

Réseau social : Les réseaux sociaux permettent à leurs membres de se bâtir un réseau de contacts à des fins personnelles ou professionnelles.

Chaque membre est invité à se créer un profil (plus ou moins élaboré, selon le site) et à y publier différents renseignements (texte, photo, vidéo, etc.) qui pourront être consultés par les gens composant son réseau de contacts et parfois, par un plus grand nombre de personnes encore (selon les paramètres de confidentialités établis par le membre concerné).

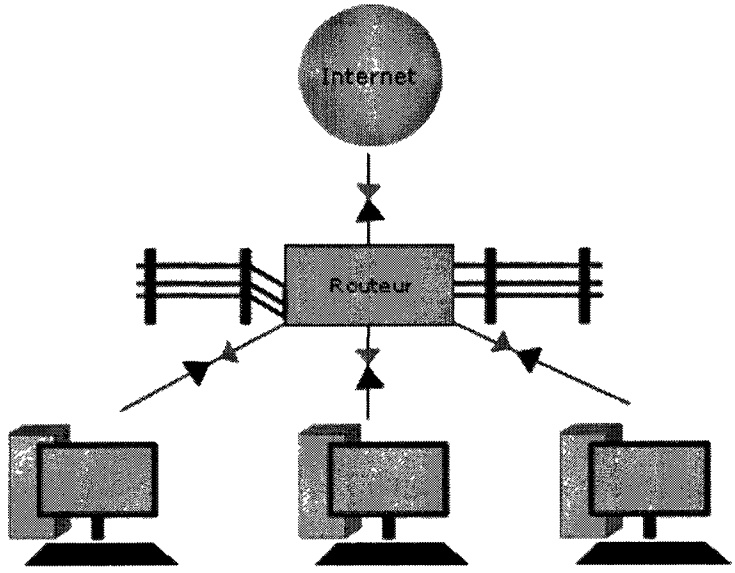
Exemples : Facebook, Twitter, MySpace, etc.

Synonyme : Média social
Anglais : *Social Network*

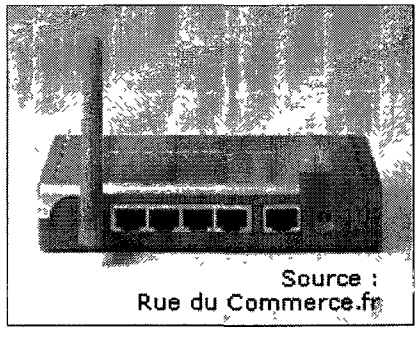
Sources : Grand dictionnaire terminologique, Wikipédia.

Routeur : À domicile, il s'agit d'un appareil permettant à plusieurs ordinateurs d'avoir accès à une seule connexion Internet et d'être accessibles à partir d'Internet.

En plus d'assurer la transmission des données, le routeur peut également agir à titre de pare-feu matériel (qu'on peut comparer à une sorte de « barrière coulissante ») grâce au logiciel qu'il contient.



Bien qu'il remplisse des tâches similaires à celles du concentrateur (*hub*), le routeur héberge un logiciel, ce qui n'est pas le cas du concentrateur.



Anglais : *Router*

Sources : Grand dictionnaire terminologique, Wikipédia.

Saisie d'écran : « Copie totale ou partielle de l'image affichée à l'écran d'un ordinateur. » (Grand dictionnaire terminologique)

Anglais : *Print screen*

Sources : Grand dictionnaire terminologique

Script : Série d'instructions simples, développées avec des langages précis, servant à automatiser certaines tâches informatiques, qu'elles soient honnêtes ou

malveillantes.

Anglais : *Script*

Sources : Grand dictionnaire terminologique, Le Jargon français

Serveur :

Dans une approche client-serveur, le serveur est un « super » ordinateur (ou un logiciel, dans le cas des serveurs virtuels) qui fournit un service en exécutant, entre autres, des requêtes formulées par des clients. Il existe différents types de serveur qui peuvent offrir :

- un accès à Internet;
- l'accès à de l'information à distance;
- la gestion d'un réseau;
- etc.

Approche client-serveur :
On peut comparer le serveur à un gros « centre de distribution » et le client, à une petite « usine de traitement ». Lorsque le serveur reçoit une requête d'un ordinateur client, il lui envoie (ou « distribue ») les données nécessaires pour répondre à cette requête. Par la suite, l'ordinateur client traite ces données pour que l'utilisateur puisse en profiter.

Anglais : *Server*

Source : Grand dictionnaire terminologique, Le Jargon français

Signature d'infection :

Les logiciels malveillants sont conçus avec plusieurs lignes de code. Parmi tout ce code se trouve une série de caractères propre à un seul logiciel malveillant; il s'agit de la signature.

De nouveaux logiciels malveillants apparaissent chaque jour. Pour être en mesure de les détecter et si possible, de les éradiquer, les logiciels antivirus et antiespiogiciels doivent **connaître** ces signatures spéciales, raison pour laquelle ils demandent des mises à jour régulières. De cette manière, ils sont au courant des dernières menaces et sont prêts à les affronter.

Certains logiciels offrent des mises à jour automatiques. Il est toutefois important de vérifier si vos logiciels offrent cette fonctionnalité.

Synonyme : Signature virale
Anglais : *Infection signature*

Source : Grand dictionnaire terminologique

Site de confiance :

Site Web reconnu comme étant fiable et sécuritaire. Il peut s'agir d'un site généraliste, d'entreprise, d'un organisme public, de téléchargement, etc.

Il est impératif de faire tous vos téléchargements à partir de sites de confiance afin d'éviter les mauvaises surprises (logiciel malveillant, vol de données, etc.). Voici quelques exemples de sites de confiance :

Téléchargements en tous genres :

- Free Download Center (anglais);
- Commentçamarche.net - Télécharger;
- Download.com (anglais).

Sites de fabricants de logiciels de sécurité :

- Avast!;
- Avira;
- Norton;
- McAfee;
- Kaspersky.

SMTP : Protocole de communication permettant l'envoi des courriels.

Acronyme de : *Simple Mail Transfer Protocol*

Source : Grand dictionnaire terminologique

Suite bureautique : Suite logicielle comprenant différents programmes utiles dans un contexte de travail. Une suite bureautique typique inclut au moins un logiciel de traitement de texte, un tableur, un logiciel de présentation, un gestionnaire de bases de données et un logiciel de courriel.

Exemples : OpenOffice, StarOffice, Microsoft Office

Anglais : *Office suite*

Sources : Grand dictionnaire terminologique, Wikipédia.

Système d'exploitation : Logiciel de base responsable de la liaison entre les ressources matérielles d'un ordinateur (carte mère, micro-processeur, disque dur, carte vidéo, etc.), les différents logiciels installés et les périphériques à l'extérieur de l'ordinateur (imprimante, écran, scanneur, etc.). Bref, il offre à l'utilisateur un environnement convivial pour manipuler son ordinateur.

Exemples :

- Récents : Windows XP, Windows Vista, Windows 7, Mac OS X Leopard (10.5), Ubuntu 9.10, etc.
- Plus anciens : Unix, MS-Dos, etc.

Comme l'ensemble des logiciels, le système d'exploitation a des brèches,

parfois petites, parfois grandes. Pour qu'elles soient « colmatées », il doit être régulièrement **mis à jour**.

Le système d'exploitation Windows propose un système de mise à jour appelé **Windows Update**. Habituellement, il est paramétré pour que les mises à jour s'installent automatiquement. Pour vous assurer que ce service s'exécute automatiquement, ou pour apporter des modifications, il est important d'accéder à la fonctionnalité Windows Update.

Pour savoir comment paramétrer la fonctionnalité Windows Update, consultez la fiche Mises à jour de Windows.

Abréviation : SE
Anglais : *Operating system, OS*

Sources : Grand dictionnaire terminologique, Wikipédia, Wikipedia.

TCP :

Protocole qui établit les connexions et contrôle la transmission des données. La paire TCP/IP est nécessaire à toute connexion Internet.

Acronyme de : *Transmission Control Protocol*

Sources : Grand dictionnaire terminologique, Wikipédia, Le Jargon français.

Témoin (*cookie*) :

Petit fichier texte installé par un serveur Web sur l'ordinateur d'un internaute lors d'une visite sur un site Web.

Des renseignements sur l'internaute (adresse courriel, nom d'utilisateur, parfois même une adresse IP) et sur ses habitudes de navigation sont enregistrés dans ce fichier. Par la suite, lorsque l'internaute reviendra sur le site, il sera reconnu et l'information affichée sera personnalisée.

En tant que tels, les témoins ne sont pas dangereux. Ils sont toutefois controversés, puisqu'ils sont installés sur un ordinateur et récoltent des renseignements à l'insu de son utilisateur.

Anglais : *Cookie*

Sources : Grand dictionnaire terminologique, Wikipédia, Le Jargon français.

Ver[illegible] :

[illegible]

Source : Wikipédia, Le Jargon français

VBS : Langage de script développé par Microsoft pour opérationnaliser certaines tâches et pour créer des applications Web dynamiques.

Certains vers informatiques sont d'ailleurs conçus avec ce langage, dont le ver *I Love You.*

Acronyme de : *Visual Basic Script*

Source : Grand dictionnaire terminologique, Wikipédia

Voix sur réseau IP : Technologie qui permet de faire passer la voix sur un réseau numérique comme Internet. On parle donc de téléphonie sur Internet.

Abréviation : VoIP
Anglais : *Voice over IP*

Sources : Grand dictionnaire terminologique, Le Jargon français

Vol d'identité : Fraude où un criminel s'empare des renseignements confidentiels d'un individu, contre son gré et généralement à son insu, afin de les utiliser à des fins illégales en se faisant passer pour l'individu lésé.

Pour en savoir plus, consultez les Questions + réponses.

Anglais : *Identity Theft*

Sources : Grand dictionnaire terminologique, Le Jargon français, Wikipédia

Web : Système sur Internet qui permet de chercher de l'information et de la consulter.

Sources : Grand dictionnaire terminologique, Le Jargon français

Web 2.0 : Expression servant à qualifier le « nouvel Internet », celui où l'usager peut prendre le contrôle de son utilisation. Il est désormais en mesure de manipuler aisément des applications Web (munies d'interfaces conviviales) pour interagir avec les contenus et avec d'autres utilisateurs.

En plus de sa dimension technologique (décrite ci-haut), le Web 2.0 a une dimension sociale, en raison de l'impact de cette nouvelle utilisation d'Internet sur une population en recherche constante de services.

Il a également un impact sur le monde des affaires, puisque bon nombre d'entreprises n'hésitent plus à inclure les technologies du Web 2.0 à leurs différentes stratégies d'affaires.

Sources : InternetACTU.net, Wikipédia.

Webmestre : Personne chargée de la création et de l'entretien d'un site Web.

Anglais : *Webmaster*

Source : Grand dictionnaire terminologique

Wiki: Type de site Web permettant aux utilisateurs de participer à la rédaction et à l'édition du contenu grâce à une interface facile à manipuler.

Anglais : *Wiki*

Sources : Grand dictionnaire terminologique, Le Jargon français

‹‹ Page précédente

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour : 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

MENACES

Une menace sur Internet, qu'est-ce que c'est? Il s'agit d'un risque **omniprésent** pouvant surgir à tout moment.

Tous les internautes sont à risque de subir les contrecoups des menaces, mais à différents degrés. En effet, un internaute bien protégé, conscient de ses responsabilités informatiques et attentif à ses actions est moins à risque qu'un utilisateur peu soucieux et trop aventureux.

Certaines menaces se présentent sous la forme de **logiciels malveillants**, de petites applications malicieuses qui peuvent être téléchargées ou encore, qui peuvent s'infilter en exploitant une faille dans un logiciel.

D'autres menaces, qu'on peut qualifier de **fraudes** et de **tromperies**, ne sont pas des logiciels, mais plutôt d'autres moyens utilisés pour arnaquer et (ou) attaquer des victimes.

Bref, on est loin du simple virus informatique. Les menaces comportent désormais de multiples facettes et sont en constante évolution. Dans un tel contexte, une meilleure connaissance des « ennemis » peut vous aider, en tant qu'internaute, à réduire le risque auquel vous êtes exposé.

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises cheminement communication et langages

Université de Sherbrooke 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

Cheval de Troie (*Trojan Horse*)

Qu'est-ce que c'est?

Pensez à la mythique guerre de Troie... La célèbre ville doit sa défaite à un cheval de bois offert par les Grecs en guise d'offrande. En réalité, il s'agissait d'un leurre contenant un groupe de soldats prêts à attaquer.

Qu'il s'agisse d'un hommage ou d'un simple signifiant, le cheval de Troie moderne est un leurre informatique. Dissimulé à l'intérieur d'un logiciel d'apparence légitime ou inoffensive (comme un faux plugiciel ou un petit jeu), il ouvre généralement une porte dérobée offrant aux pirates un accès direct à l'ordinateur infecté. Il peut également exécuter des actions à l'insu de l'utilisateur floué et déclencher le téléchargement d'autres logiciels malveillants.

Plus >>

Comment prévenir et comment guérir?

Les logiciels antivirus et certains logiciels antiespiogiciels sont en mesure de détecter ces dangereux parasites et parfois de les éradiquer, si leurs signatures d'infection sont à jour. De plus, l'installation d'un pare-feu permet de limiter les accès impromptus.

Les chevaux de Troie constituent l'une des menaces les plus problématiques sur Internet, majoritairement en raison de la porte dérobée qu'ils ouvrent. Cet accès camouflé permet aux pirates de s'imposer dans aucune limite, qu'il s'agisse d'afficher un simple « Coucou! » ou de voler une foule de renseignements confidentiels.

La guerre n'étant jamais bien loin de votre ordinateur, mieux vaut vous protéger contre d'éventuelles attaques avec les logiciels adéquats et une bonne dose de vigilance!

Plus >>

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises cheminement communication et langages

Université de Sherbrooke 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Cheval de Troie (*Trojan Horse*)

1. Qu'est-ce que c'est?

À l'image du mythique cheval de bois, le cheval de Troie est un programme malveillant qui se dissimule à l'intérieur d'un autre programme en apparence inoffensif (comme un petit jeu ou un faux plugiciel).

Lorsque le bon programme est téléchargé, le mauvais l'est également. Généralement, le cheval de Troie ouvre une porte dérobée destinée aux pirates souhaitant accéder à l'ordinateur infecté. Ils peuvent alors y agir comme bon leur semble et prendre le contrôle de l'ordinateur, que ce soit à 10 % (afficher un petit message à l'écran) ou à 100 % (contrôler toutes les actions exécutées).

Les chevaux de Troie peuvent également exécuter plusieurs actions à l'insu de l'utilisateur floué et activer l'installation d'autres logiciels malveillants, comme des espiogiciels, des faux logiciels de sécurité, etc.

<< Retour

2. Comment ça fonctionne?

La particularité du cheval de Troie est son camouflage sous des habits de logiciel d'apparence légitime. Il peut être téléchargé consciemment par un internaute peu vigilant, par exemple lorsqu'il est dissimulé dans un petit jeu gratuit et bien tentant. Mais il peut également s'infiltrer par une faille dans un logiciel, et ce, à l'insu de l'utilisateur.

Peu importe son mode d'infiltration, il cherche à rester le plus discret possible pour étendre la durée de ses actions.

Ces actions dépendent d'ailleurs de sa programmation originale. Certains vont se concentrer sur l'ouverture d'une porte dérobée pour permettre à un (ou plusieurs) pirate de s'introduire dans l'ordinateur infecté en toute liberté. En guise d'analogie, c'est un peu comme si un criminel s'infiltrait dans votre maison et en profitait pour inviter d'autres malfrats, tout ça à votre insu.

D'autres ont plutôt l'objectif de recueillir des renseignements confidentiels et mettront tout en oeuvre pour y arriver (utilisation d'un enregistreur de frappe, surveillance d'un pirate, etc.).

Bref, les actions des chevaux de Troie dépendent de leurs objectifs, aussi diversifiés que les intentions des pirates qui les utilisent.

<< Retour

3. Quelles en sont les conséquences?

Les conséquences d'un cheval de Troie dépendent de sa programmation originale. La porte dérobée peut donner accès à votre ordinateur à un ou plusieurs pirates, qui en prendront le contrôle et feront ce qu'ils veulent : afficher un petit « Coucou! » sur votre écran, consulter ou supprimer de données, voler des renseignements confidentiels, etc.

Le cheval de Troie peut également ouvrir le chemin à d'autres logiciels malveillants, comme des espiogiciels, des faux logiciels de sécurité, etc. Dans ce cas, tous les inconvénients de ces parasites sont combinés à ceux des chevaux de Troie.

<< Retour

4. Des exemples

Un exemple? Le cheval de Troie Back Orifice a connu la « gloire » en 1999. Il permettait une prise de contrôle totale et à distance d'un ordinateur, tout ça dans une optique malveillante. La deuxième version de ce cheval de Troie, affectueusement surnommée BO2, était même en mesure d'infecter les serveurs pour une prise de contrôle éventuelle.

Un autre exemple? Le cheval de Troie Openstream.T, découvert au début de l'année 2005, se téléchargeait sur un ordinateur par l'intermédiaire d'une page Web piégée contenant un applet Java. Lorsque l'applet Java était exécuté, il téléchargeait le vilain cheval de Troie, qui à son tour déclenchait l'installation de divers logiciels malveillants. Heureusement pour les internautes, il n'a pas fait beaucoup de dommages, puisque son installation n'était pas automatique; il fallait d'abord accepter l'exécution de l'applet Java, ce que plusieurs internautes conscientisés n'ont pas fait.

Un dernier exemple? En juin 2009, le cheval de Troie OSX/Jahlav-C a défrayé les manchettes des journaux techno. Il s'est propagé en utilisant la page Twitter du populaire Guy Kawasaki, grand prêcheur des ordinateurs MacIntosh, et ciblait justement les ordinateurs MacIntosh, ce qui était assez exceptionnel en soi. Sous la promesse d'une vidéo érotique mettant en vedette une actrice américaine, les victimes appâtées cliquaient sur un hyperlien menant ultimement au téléchargement du logiciel malveillant. Ce cheval de Troie a causé des dommages d'une certaine importance, puisque plusieurs de ses victimes (utilisant un ordinateur MacIntosh) n'avaient installé aucun logiciel de sécurité. Une telle position est à réévaluer, car aujourd'hui aucun ordinateur connecté à

Internet n'est inatteignable, peu importe son système d'exploitation.

<< Retour

5. Comment prévenir?

Plusieurs logiciels sont impliqués dans la protection contre les chevaux de Troie :

- Un pare-feu correctement paramétré;
- Un logiciel antivirus activé en tout temps et dont les signatures d'infection sont à jour;
  - Pensez à l'activer en tout temps et à scanner votre ordinateur au moins deux fois par mois.
- Au moins deux logiciels antiespiogiciels dont les signatures d'infection sont à jour;
  - Pensez à scanner votre ordinateur avec chaque antiespiogiciel au moins une fois par semaine.

ATTENTION :

Scanner votre ordinateur plusieurs fois par semaine avec chaque antiespiogiciel peut être nécessaire si :

- Votre ordinateur est ouvert et connecté à Internet durant de longues heures; ou
- Vous faites beaucoup de téléchargement (en tous genres).

- Votre système d'exploitation, il doit être à jour;
- Votre navigateur, il doit être à jour;
- Votre logiciel de courriel (si vous en utilisez un), il doit être à jour;
- Votre tête, car la vigilance est de mise!

ATTENTION

Vous avez reçu courriel contenant un fichier exécutable (avec l'extension .EXE, .COM, .CMD ou .BAT) en pièce jointe, agrémenté d'un message vous incitant fortement à l'ouvrir? Attention! Il pourrait s'agir d'un cheval de Troie! N'ouvrez pas un fichier exécutable en pièce jointe à un courriel, ce n'est jamais de bon augure.

Vous êtes tombé sur un site Web dont la fiabilité ne peut être prouvée et qui offre des petits utilitaires si intéressants? Encore une fois, attention! Un cheval de Troie pourrait se trouver parmi ces petits logiciels. Assurez-vous de télécharger des logiciels à partir de sites de confiance.

<< Retour

6. Comment guérir?

Vous êtes infecté par un cheval de Troie? Voici ce que vous pouvez faire.

1. Installez tout de suite un pare-feu, pour éviter que ne problème ne prenne de l'ampleur.
2. Analysez votre ordinateur avec un logiciel antivirus.
   Supprimez les menaces détectées, s'il y en a.
3. Analysez votre ordinateur avec un logiciel antiespiogiciel .
   Supprimez les menaces détectées, s'il y en a.
4. Analysez votre ordinateur avec un deuxième logiciel antiespiogiciel.
   Supprimez les menaces détectées, s'il y en a.
5. Si malgré toutes ces analyses le cheval de Troie subsiste, faites ceci :
   a. Redémarrez votre ordinateur en mode sans échec.
   b. Faites une analyse antivirus. Supprimez les menaces détectées, s'il y en a.
   c. Faites une analyse antiespiogicielle (avec un logiciel antiespiogiciel). Supprimez les menaces détectées, s'il y en a.
   d. Redémarrez votre ordinateur en mode Normal.
6. Certains chevaux de Troie sont plus tenaces alors, s'il est toujours là malgré toutes ces analyses, vous devrez faire un peu de recherche...
   a. Notez le nom du cheval de Troie tel qu'il vous est apparu la première fois, lorsqu'un logiciel vous a signalé sa détection. Prenez également note des symptômes éprouvés par votre ordinateur.
   b. Allez sur ce site, Commentçamarche.net. Cette communauté informatique offre des forums de discussion où une foule de gens, des professionnels du milieu ou des internautes munis d'une solide expérience dans le domaine, sont prêts à vous aider en tout temps.
   c. Tapez le nom du cheval de Troie, ou les symptômes notés, dans la zone de recherche. N'hésitez pas à poser des questions si vous ne trouvez pas une réponse qui vous convient!

Un grand sage a un jour dit : « Si ça vous arrive, c'est sûrement déjà arrivé à quelqu'un d'autre... Et cette autre personne a certainement cherché une réponse dans un forum. » ;-)

<< Retour

7. Sources documentaires

- Assiste.com
- Branchez-vous.com
- Grand dictionnaire terminologique
- Le Jargon français
- Secuser.com
- Wikipédia (français)
- GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition,* coll. « microapp », Paris,

Micro Application, 2007, 1247 p.

- GRALLA, Preston. *PC Pest Control*, Sebastopol, O'Reilly Media Inc., 2005, 275 p.
- LEVINE, John R. *Sécurité Internet pour les nuls*, Paris, Éditions First Interactive, 2003, 398 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet
Maîtrise en études françaises, cheminement communication et langages
Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

Espiogiciel (*Spyware*)

Qu'est-ce que c'est?

Imaginez le scénario suivant. Vous vaquez à vos occupations habituelles et vous êtes bien concentré sur ce que vous faites. Pendant ce temps, un vilain petit espion, tout de noir vêtu, se cache dans un coin et épie chacun de vos gestes : ce que vous lisez, ce que vous écrivez, qui vous appelez... Tout ça sans votre autorisation.

L'espiogiciel agit de la même manière : il s'infiltre dans votre ordinateur à votre insu et épie chacun de vos gestes informatiques. Il peut ensuite utiliser les renseignements recueillis comme bon lui semble, souvent à des fins publicitaires.

Les espiogiciels sont malheureusement très nombreux sur Internet. D'un point de vue technologique, c'est surtout en nombre qu'ils sont nuisibles; plus il y en a, plus votre ordinateur éprouvera des difficultés. D'un point de vue éthique, ils sont plus que douteux, puisque leurs agissements peuvent compromettre la vie privée des internautes.

Plus >>

Comment prévenir et comment guérir?

Pour éradiquer les espiogiciels, il importe d'utiliser au moins deux logiciels antiespiogiciels. La procédure à suivre est simple : les installer, mettre religieusement à jour leurs signatures d'infection et scanner l'ordinateur au moins une fois par semaine avec chaque antiespiogiciel.

De plus, l'installation pare-feu est requise, de même que son paramétrage. L'utilisation d'un logiciel « de ménage » peut également être utile pour nettoyer la base de registre. En effet, certains espiogiciels tenaces arrivent à s'inscrire dans la base de registre pour être en mesure de s'installer de nouveau en cas de suppression.

Bien que ces logiciels soient d'une aide précieuse, la vigilance est de mise pour prévenir l'infiltration d'espiogiciels. Laissez tomber les téléchargements illégaux et si vous fréquentez des sites chargés de publicités, braquez derrière un bon pare-feu et une protection antiespiogicielle en temps réel.

Plus >>

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Espiogiciel (*Spyware*)

1. Qu'est-ce que c'est?

Tel que mentionné à la page précédente, l'espiogiciel est comme un petit espion, tout de noir vêtu, épiant chacun de vos gestes dans l'objectif ultime de placarder chaque mur de votre maison avec des publicités en tous genres.

Sournois et discret, il cherche à répertorier ce que vous faites : l'historique de votre navigation, les témoins installés sur votre ordinateur, la liste de vos favoris, votre adresse IP, etc.

Une fois les données rassemblées, il les envoie à une tierce personne, encore une fois à votre insu. Cette tierce personne est parfois une entreprise, parfois un seul individu, et elle pourra utiliser ces renseignements à des fins de ciblage comportemental.

<< Retour

2. Comment ça fonctionne?

Comme il a été mentionné ci-haut, l'espiogiciel a pour but d'enregistrer les activités d'un internaute à son insu en consultant l'historique de votre navigation, les témoins installés, la liste de vos favoris, l'adresse IP, etc. Certains espiogiciels vont encore plus loin en sauvegardant les recherches effectuées dans un moteur de recherche.

Ensuite, selon les données recueillies, un profil d'internaute sera dressé. Ce profil permettra de personnaliser la publicité affichée sur son écran d'ordinateur en fonction de ses besoins et de ses

intérêts. Toute cette publicité pourra s'afficher non seulement pendant sa navigation (dans des fenêtres pop-up, les espaces publicitaires, etc.), mais également lors d'autres activités, tant que l'ordinateur est actif et connecté. Toute cette publicité ne sert qu'un seul objectif : **gagner** de l'argent.

Étant donné la popularité des espiogiciels dans le monde publicitaire, il arrive malheureusement que certains soient utilisés à des fins malveillantes. Des renseignements peuvent être recueillis à des fins de vol (numéro de carte de crédit, mots de passe, renseignements confidentiels) et ils sont utilisés pour vous voler. L'objectif est alors de **voler** de l'argent.

Ces petits colporteurs binaires sont passés maîtres dans l'art de contourner les protections et réussissent à s'installer à l'insu de l'usager. Le procédé d'installation, voire d'implantation, est sournois... et pourtant simple, puisqu'il cible souvent le manque de vigilance des internautes et leurs autres faiblesses. Par exemple, tout individu téléchargeant illégalement des fichiers audio ou vidéo avec un logiciel de pair à pair se met en position risquée. En effet, ce type de logiciel ouvre plusieurs ports pour permettre les téléchargements et ces ports ne sont pas toujours sécurisés. Plusieurs parasites peuvent alors s'infiltrer. Et il ne faut pas négliger la quantité de fichiers corrompus et malicieux (logiciels malveillants, ou fichiers sains auxquels sont greffés des parasites) qui circulent sur les réseaux des logiciels de pair-à-pair.

ATTENTION

Les procédés d'installation des espiogiciels se perfectionnent au rythme de l'évolution d'Internet. Depuis quelques années, certains espiogiciels s'installent sans aucune intervention de l'utilisateur; ils exploitent plutôt les failles d'un logiciel, qu'il s'agisse du système d'exploitation, du navigateur ou d'un autre logiciel populaire. Une protection en temps réel devient alors pertinente, au meilleur de ses capacités, contre ce type de téléchargement automatique.

<< Retour

3. Les types d'espiogiciels

Il existe différents types d'espiogiciels dont il faut se protéger. Il y a le « standard », qui épie chacun de vos gestes informatiques, et il y en a d'autres :

a. ***L'enregistreur de frappe (*Keylogger*)***

Comme son nom le suppose, l'enregistreur de frappe a pour mission d'enregistrer, dans un fichier texte, toutes les touches qui sont enfoncées sur le clavier, et ce, afin de récupérer des données intéressantes comme des mots de passe, des noms d'utilisateur, des renseignements bancaires, etc. Certaines variantes d'enregistreurs de frappe peuvent également noter les sites Web visités, les courriels reçus et envoyés et les fichiers ouverts.

Par la suite, les données recueillies peuvent servir soit à envoyer de la publicité personnalisée, soit à commettre un vol...

CULTURE GÉNÉRALE

Il existe des enregistreurs de frappe parfaitement légaux et majoritairement utilisés en entreprise pour surveiller les activités des employés.

b. ***Le* browser hijacker**

Ce type d'espiogiciel cherche à modifier la page d'accueil du navigateur de l'internaute pour programmer l'affichage d'une autre page.

Dans un contexte publicitaire, le *browser hijacker* va imposer l'affichage d'une page précise, ce qui fera augmenter le nombre de visites sur le site en question.

QUESTION

« Pour quelle raison voudrait-on augmenter le trafic sur un site Web? » Pour des considérations financières : plus un site Web est visité, plus il a un potentiel publicitaire rentable.

Dans un contexte malveillant, le *browser hijacker* peut imposer l'affichage d'une page piégée, truffée de publicités, de fenêtres pop-up ou pire, de logiciels malveillants.

<< Retour

4. Quelles en sont les conséquences?

D'un point de vue technologique, lorsqu'un ordinateur est infecté par plusieurs espiogiciels, son fonctionnement est ralenti, que ce soit de manière subtile ou considérable.

Un seul espiogiciel ne peut pas ralentir un système, mais 100 espiogiciels peuvent le rendre totalement inutilisable.

D'un point de vue humain, lorsqu'un ordinateur est infecté par un ou plusieurs espiogiciels, cela signifie qu'il y a un risque de vol de données, ce qui peut mener à un vol d'argent ou pire, d'identité.

Un seul espiogiciel peut alors causer de sérieuses pertes.

On comprend donc que les espiogiciels sont éthiquement douteux, sans oublier que leurs conséquences technologiques peuvent être agaçantes, irritantes, voire choquantes. Toutefois, comme il a été mentionné ci-haut, ils sont rentables donc, ils ne sont pas près de disparaître. Alors, chers internautes, blindez votre machine!

<< Retour

5. Des exemples

Un exemple? On ne peut pas parler d'espiogiciels sans observer de plus près le phénomène KaZaA, qui a littéralement laissé sa trace dans l'histoire d'Internet. Le logiciel de pair-à-pair, qui permettait le partage de fichiers en tous genres, n'était pas un espiogiciel en soi, mais il en véhiculait tellement

qu'il a été perçu comme un espiogiciel redoutable. Ainsi, à lui seul, il aurait probablement propagé plusieurs milliards d'espiogiciels de toutes sortes, ce qui le rendait particulièrement rentable pour son propriétaire, Sharman Networks, mais très désagréable pour ses millions d'utilisateurs.

Un autre exemple? L'espiogiciel Gator, lancé en 1998, est peu actif aujourd'hui, mais il est toujours « vivant ». Il était l'un des espiogiciels greffés au logiciel KaZaA et il s'était également joint à d'autres logiciels de pair-à-pair. Son but était d'observer les activités de l'utilisateur, puis d'acheminer les données recueillies au propriétaire, l'entreprise Gator, désormais connue sous le nom de Claria Corporation. Par la suite, de la publicité était envoyée sur l'ordinateur de la victime et la page d'accueil de son navigateur était modifiée.

CULTURE GÉNÉRALE

Selon Claria Corporation, Gator aurait été installé sur un total de 43 millions d'ordinateurs, entre 1998 et 2005.

Un dernier exemple? Certains espiogiciels ont pour but de modifier toutes les publicités présentées à l'internaute, peu importe le site sur lequel il se trouve. Ils emploient ce moyen détourné, car les entreprises qui les ont conçus œuvrent souvent dans des domaines où elles n'ont pas le droit de distribuer librement de la publicité (par exemple, dans le domaine de la pornographie). Si un ordinateur est infecté par l'un de ces espiogiciels, il se peut donc que le résultat soit légèrement... déroutant. Par exemple, si un internaute navigue parfois sur des sites pornographiques et qu'un tel espiogiciel s'infiltre dans son système, il est possible que son site de nouvelles préféré lui affiche désormais des publicités quelque peu lubriques.

<< Retour

6. Comment prévenir?

Plusieurs logiciels sont impliqués dans la protection contre les espiogiciels :

- Au moins deux logiciels antiespiogiciels dont les signatures d'infection sont à jour;
    - Pensez à scanner votre ordinateur avec chaque antiespiogiciel au moins une fois par semaine.

      ATTENTION :

      Scanner votre ordinateur plusieurs fois par semaine avec chaque antiespiogiciel peut être nécessaire si :
        - Votre ordinateur est ouvert et connecté à Internet durant de longues heures; ou
        - Vous faites beaucoup de téléchargement (en tous genres).

- Un pare-feu correctement paramétré;
- Un logiciel « de ménage », pour nettoyer à la fois votre ordinateur des éléments qui pourraient « nourrir » les espiogiciels, et la base de registre;
    - Pensez à scanner votre ordinateur et votre base de registre au moins une fois par

semaine.

- Une protection antiespiogicielle en temps réel;
- Votre système d'exploitation, il doit être à jour;
- Votre navigateur, il doit être à jour;
- Votre logiciel de courriel (si vous en utilisez un), il doit être à jour;
- Votre tête, car la vigilance est de mise!

ATTENTION

Dans plusieurs cas, lorsqu'un ordinateur est infecté par des espiogiciels, c'est souvent parce que la protection de base est soit absente, soit inadéquate. Le problème va donc au-delà de la technologie, jusqu'à 18 pouces derrière l'écran. En tant qu'internaute, vous devez être **conscient** de vos actes sur le réseau :

- Vous aimez naviguer sur des sites de réseautage social contenant beaucoup de publicité, comme Facebook? Les risques d'affichage publicitaire et de vol de renseignements confidentiels sont élevés, vous aurez besoin d'abord d'un maximum de protection (un pare-feu, deux espiogiciels, une protection antiespiogicielle en temps réel, et un système d'exploitation et un navigateur à jour), mais surtout d'une bonne dose de **vigilance**.

- Vous faites des téléchargements à partir de sources non fiables, comme les logiciels de pair-à-pair (*peer-to-peer*)? Les risques d'affichage publicitaire et de vol de données sont très élevés, vous aurez besoin d'un maximum de protection (un pare-feu, deux espiogiciels, une protection antiespiogicielle en temps réel, et un système d'exploitation et un navigateur à jour) et d'une immense dose de **vigilance**.

  De plus, si vous tenez mordicus aux téléchargements de pair-à-pair, n'oubliez pas qu'utiliser ces logiciels est non seulement dangereux, mais potentiellement illégal, car ils véhiculent bon nombre de fichiers illégaux. Mieux vaut alors opter pour des solutions moins risquées, quitte à investir quelques dollars (par exemple, iTunes offre des chansons à 1 $).

<< Retour

7. Comment guérir?

Vous êtes infecté par un espiogiciel? Voici ce que vous pouvez faire.

1. Installez tout de suite un pare-feu, pour éviter que ne problème ne prenne de l'ampleur.
2. Analysez votre ordinateur avec un logiciel antiespiogiciel .

Supprimez les menaces détectées, s'il y en a.

3. Analysez votre ordinateur avec un deuxième logiciel antiespiogiciel.
   Supprimez les menaces détectées, s'il y en a.
4. Passez un petit coup de balai avec un logiciel « de ménage ».
   Supprimez les résidus détectés.
5. Si malgré toutes ces analyses l'espiogiciel subsiste, faites ceci
   a. Redémarrez votre ordinateur en mode sans échec.
   b. Faites une analyse antiespiogicielle (avec un logiciel antiespiogiciel). Supprimez les menaces détectées, s'il y en a.
   c. Redémarrez votre ordinateur en mode Normal.
6. Certains espiogiciels sont plus tenaces alors, s'il est toujours là malgré toutes ces analyses, vous devrez faire un peu de recherche...
   a. Notez le nom de l'espiogiciel tel qu'il vous est apparu la première fois, lorsqu'un logiciel vous a signalé sa détection.
   b. Allez sur ce site, Commentçamarche.net. Cette communauté informatique offre des forums de discussion où une foule de gens, des professionnels du milieu ou des internautes munis d'une solide expérience dans le domaine, sont prêts à vous aider en tout temps.
   c. Tapez le nom de l'espiogiciel dans la zone de recherche. N'hésitez pas à poser des questions si vous ne trouvez pas une réponse qui vous convient!

Un grand sage a un jour dit : « Si ça vous arrive, c'est sûrement déjà arrivé à quelqu'un d'autre... Et cette autre personne a certainement cherché une réponse dans un forum. » ;-)

<< Retour

8. Sources documentaires

- Assiste.com
- Grand dictionnaire terminologique
- Internet Security Zone.com
- Le Jargon français
- Wikipédia (français)
- Wikipédia (anglais)
- CHARTON, ÉRIC. *Spywares et virus : Protégez-vous des logiciels escrocs*, coll. « Kit Campus », Paris, CampusPress, 2005, 245 p.
- GRALLA, Preston. *PC Pest Control*, Sebastopol, O'Reilly Media Inc., 2005, 275 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

Faux logiciel de sécurité (*Rogue Security Software*)

Qu'est-ce que c'est?

Un faux logiciel de sécurité est, comme son nom l'indique, un logiciel qui paraît vous protéger contre différents logiciels malveillants, mais qui en réalité ne le fait pas du tout. Sa présence peu subtile peut se caractériser par :

- des alertes incessantes et alarmantes (par exemple : 428 virus ont été détectés sur votre ordinateur!);
- des demandes d'analyse fréquentes;
- la modification de certains paramètres du système d'exploitation;
- l'affichage de fenêtres pop-up;
- etc.

Lorsqu'un faux logiciel de sécurité s'installe, il est extrêmement difficile de le supprimer. Plus il reste longtemps sur un ordinateur, plus il peut agir sur une longue période. Il obtient alors la latitude nécessaire pour faire paniquer un utilisateur avec de fausses alertes et de faux résultats, et pour l'inciter à poser une action ultimement rentable pour le pirate derrière le faux logiciel.

Plus >>

Comment prévenir et comment guérir?

Les faux logiciels de sécurité circulent un peu partout sur Internet et peuvent s'infiltrer dans un ordinateur de différentes manières. Ils peuvent utiliser les « services » d'autres parasites, se propager par un pourriel, ou encore exploiter une faille dans un logiciel. L'installation et le paramétrage d'un pare-feu, de même que la mise à jour régulière du système d'exploitation et du navigateur offrent alors une bonne protection. Il ne faut pas négliger les autres logiciels de sécurité, comme l'antivirus, l'antiespiogiciel et l'*antirootkit*, qui sont en mesure de bloquer tout parasite pouvant propager un faux logiciel de sécurité.

Cependant, ils peuvent aussi s'installer à la suite d'un clic imprudent sur une publicité trompeuse. Il est important d'éviter tout clic spontané sur des publicités, aussi invitantes soient-elles. En effet, certaines ressemblent à s'y méprendre à différentes alertes de Windows, ou à des messages d'apparence légitime provenant d'un logiciel de sécurité.

Toutefois, s'il est trop tard, pas de panique. Pour tenter de l'éradiquer, vous aurez besoin d'un pare-feu, d'un logiciel antivirus et d'au moins deux logiciels antiespiogiciels dont les signatures

d'infection sont à jour, sans oublier une bonne dose de patience.

Plus >>

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour : 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurite Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Faux logiciel de sécurité (*Rogue Security Software*)

1. Qu'est-ce que c'est?

Les faux logiciels de sécurité ont plus d'un tour dans leur sac. Comme leur nom le suppose, ils sont faux : leurs analyses, leurs résultats, les alertes qu'ils affichent, tout est falsifié. Leur objectif ultime est d'obtenir de l'argent avec une fraude parfois grossière, mais parfois très habile et surtout, organisée.

On pourrait penser que ces faux logiciels sont facilement identifiables, que leur apparence est sommaire ou bâclée ou qu'ils plantent à tout bout de champ. Malheureusement, il n'en est rien. Bien que quelques-uns d'entre eux soient de piètre qualité, la majorité surprennent par leur apparence convaincante et leur stabilité de fonctionnement. Pour renforcer leur crédibilité, certains n'hésitent pas à voler des logos et d'autres aspects de design à Windows ou aux grands concepteurs de logiciels de sécurité. Ils peuvent également se doter d'un nom qui inspire la confiance, comme Windows System Defender (semblable à Windows Defender), PC Security 2009, etc.

On entend parfois qu'Internet est un lieu dangereux et qu'il faut se méfier de tout ce qu'on y voit. Le faux logiciel de sécurité en est un bon exemple : malgré son **apparence** rassurante et sécuritaire, il est un réel danger pour les ordinateurs et leurs utilisateurs.

QUESTION

> « Mais si ces logiciels sont si crédibles, comment puis-je savoir s'il s'agit d'un faux logiciel ou d'un vrai? » Plusieurs signes qui peuvent vous mettre la puce à l'oreille.
>
> - Tactiques utilisées par les faux logiciels pour créer un sentiment de panique.
>
> N'oubliez pas d'utiliser votre « gros bon sens ». Les vrais producteurs de logiciels de sécurité n'ont pas besoin de publicités alarmistes et invasives pour faire connaître leurs produits. Si un logiciel vous est présenté de cette manière, il y a de fortes chances pour que ce soit une arnaque.

<< Retour

2. Comment ça fonctionne?

Les faux logiciels de sécurité ne s'installent pas sur un ordinateur par magie. Parfois, ils collaborent avec d'autres logiciels malveillants, comme les chevaux de Troie, pour soit s'installer de force, soit vous afficher de la publicité qui vous incitera à entamer leur téléchargement.

Ils peuvent également être propagés par des envois massifs de pourriels, mais cette méthode de contamination est désormais moins efficace, puisque les internautes s'en méfient de plus en plus.

Ils peuvent aussi exploiter « par eux-mêmes » une faille dans un logiciel (comme le navigateur, le système d'exploitation, etc.) pour s'infiltrer dans un système.

Malgré toutes ces « prouesses » technologiques pour arriver à infecter des ordinateurs, il arrive fréquemment qu'ils soient installés par des utilisateurs peu vigilants et aux clics trop aventureux. En effet, un simple clic sur une publicité trompeuse peut mener au téléchargement d'un ou de plusieurs logiciels de sécurité.

Une fois installé, leur objectif principal est de susciter, chez les internautes débutants ou peu conscients de leur sécurité, un **sentiment de panique** qui les incitera à poser une action : payer pour obtenir une fausse protection (ou une soi-disant réparation), entamer un téléchargement (souvent d'un ou de plusieurs parasites), ou encore laisser le faux logiciel sur l'ordinateur pour lui permettre de recueillir une foule de renseignements confidentiels. Peu importe l'action, elle est rentable pour le pirate derrière cette arnaque.

Pour créer ce sentiment de panique, le faux logiciel peut :

- Afficher des résultats de fausses analyses, résultats qui peuvent être particulièrement alarmants :
    - ATTENTION, 428 virus ont été détectés sur votre ordinateur!
    - 145 espiogiciels sont présentement actifs sur votre ordinateur, supprimez-les.

    QUESTION

    « Faut-il s'inquiéter des résultats présentés par ces logiciels? Car même s'ils sont faux, ils peuvent être convaincants... » En effet, les résultats présentés par les faux logiciels de sécurité peuvent être alarmants et il est facile de croire que grâce à ce logiciel, un ordinateur pourra être sauvé de centaines de parasites. Toutefois, c'est rarement le cas.

    En majorité, les logiciels malveillants soi-disant détectés sont des faux positifs, c'est-à-dire des parasites qui, en réalité, ne se trouvent pas sur l'ordinateur ou qui n'existent tout simplement pas.

- Demander constamment à l'utilisateur d'effectuer une analyse de son système sur-le-champ.

- Modifier des paramètres du système d'exploitation. Par exemple, il pourrait changer l'image du fond d'écran par une image alarmiste affichant un message semblable à celui-ci : Vous devez immédiatement analyser votre ordinateur, vous pourriez être en danger!
- Afficher des fenêtres pop-up en tous genres.
- Démarrer automatiquement de fausses analyses qui ralentissent le fonctionnement de l'ordinateur.
- Demander à l'utilisateur de payer pour protéger ou guérir son système ou pire, pour désinstaller le faux logiciel.
- Désactiver les mesures de sécurité en place sur l'ordinateur (comme Windows Update).
- Utiliser la fraude psychologique pour recueillir les renseignements personnels de l'utilisateur.
- Et (malheureusement) plus encore.

Il est extrêmement difficile de supprimer un faux logiciel de sécurité, car ces derniers sont faits pour rester sur un système. En effet, plus ils y restent longtemps, plus ils pourront exploiter l'ordinateur ou son utilisateur sur une longue période.

<< Retour

3. Quelles en sont les conséquences?

Une des conséquences des faux logiciels de sécurité est le **stress** inutile qu'il procure, sans oublier le temps perdu à tenter de le supprimer. Ils peuvent aussi solliciter de manière exagérée les ressources d'un ordinateur et en ralentir le fonctionnement normal.

Certains faux logiciels de sécurité partiront à la recherche de renseignements confidentiels, ou encore ils téléchargeront d'autres parasites qui se chargeront de cette collecte, tout en créant un joli bordel dans l'ordinateur infecté. Les malfaiteurs pourront alors vendre ces renseignements ou les utiliser à leur propre sauce pour, par exemple, envoyer de la publicité ou commettre un vol d'argent ou d'identité.

<< Retour

4. Comment prévenir?

Plusieurs logiciels sont impliqués dans la protection contre les faux logiciels de sécurité :

- Un « vrai » logiciel antivirus dont les signatures d'infection sont à jour;
  - Pensez à l'activer en tout temps et à scanner votre ordinateur au moins deux fois par mois.
- Un pare-feu correctement paramétré;
- Au moins deux « vrais » logiciels antiespiogiciels dont les signatures d'infection sont à jour;
  - Pensez à scanner votre ordinateur avec chaque antiespiogiciel au moins une fois par semaine.

ATTENTION :

Scanner votre ordinateur plusieurs fois par semaine avec chaque antiespiogiciel peut être nécessaire si :

- Votre ordinateur est ouvert et connecté à Internet durant de longues heures; ou
- Vous faites beaucoup de téléchargement (en tous genres).

- Votre système d'exploitation, il doit être à jour;
- Votre navigateur, il doit être à jour;
- Votre logiciel de courriel (si vous en utilisez un), il doit être à jour;
- Votre tête, car la vigilance est de mise! Utilisez votre « gros bon sens »... Si un logiciel vous semble suspect, notez son nom et vérifiez s'il fait partie d'un répertoire de faux logiciels de sécurité comme :
  - Liste d'Assiste.com;
  - Blogue de sécurité de Bharath (anglais);
  - Blogue Malwarebytes (anglais).

<< Retour

5. Comment guérir?

Vous savez que vous êtes infecté par un ou plusieurs faux logiciels de sécurité? Voici quelques solutions :

ATTENTION

Les mécanismes des faux logiciels de sécurité changent fréquemment pour éviter la suppression. Par exemple, certains faux logiciels seront ajustés tous les mois avec de nouvelles fonctionnalités qui compliqueront la tâche aux victimes souhaitant s'en débarrasser.

Par conséquent, il se peut que les solutions proposées ci-dessous ne fonctionnent pas parfaitement; il est alors très important de se tourner vers les répertoires de faux logiciels de sécurité (comme le blogue Malwarebytes - anglais) et les forums (comme Commentçamarche.net) pour trouver une solution adéquate.

1. Installez un pare-feu, pour éviter que le problème ne prenne de l'ampleur.
2. Créez un point de restauration dans Windows, au cas où les choses tourneraient mal.
3. Installez un logiciel de désinstallation et utilisez-le pour supprimer le faux logiciel. Si vous n'y arrivez pas, ne vous inquiétez pas et passez à l'étape 3.
4. Analysez votre ordinateur avec un logiciel antivirus.
   Supprimez les menaces détectées, s'il y en a.
5. Si ça ne fonctionne pas, analysez votre ordinateur avec un logiciel antiespiogiciel.
   Supprimez les menaces détectées, s'il y en a.

6. Analysez votre ordinateur avec un deuxième logiciel antiespiogiciel.
   Supprimez les menaces détectées, s'il y en a.
7. Si malgré toutes ces analyses le faux logiciel de sécurité subsiste, faites ceci
   a. Redémarrez votre ordinateur en mode sans échec.
   b. Faites une analyse antiespiogicielle (avec un logiciel antiespiogiciel) et une analyse antivirus. Supprimez les menaces détectées, s'il y en a.
   c. Redémarrez votre ordinateur en mode Normal.
8. Certains faux logiciels sont plus tenaces alors, s'il est toujours là malgré toutes ces analyses, vous devrez faire un peu de recherche...
   a. Notez le nom du faux logiciel de sécurité.
   b. Allez sur ce site, Commentçamarche.net. Cette communauté informatique offre des forums de discussion où une foule de gens, des professionnels du milieu ou des internautes munis d'une solide expérience dans le domaine, sont prêts à vous aider en tout temps.
   c. Tapez le nom de du faux logiciel dans la zone de recherche. N'hésitez pas à poser des questions si vous ne trouvez pas une réponse qui vous convient!

      Un grand sage a un jour dit : « Si ça vous arrive, c'est sûrement déjà arrivé à quelqu'un d'autre... Et cette autre personne a certainement cherché une réponse dans un forum. » ;-)

      Vous pouvez toujours poser des questions aux administrateurs des blogues de Bharath et Malwarebytes, mais ils doivent être suffisamment occupés avec la mise à jour constante de leur blogue, peut-être ne pourront-ils pas vous répondre dans les délais souhaités. Mieux vaut alors de tourner vers un forum.

<< Retour

6. Sources documentaires

- Assiste.com
- Blogue de sécurité de Bharath (anglais)
- Blogue Malwarebytes (anglais)
- Microsoft Security (anglais)
- Technaute - Blogue de Nelson Dumais
- Wikipedia (anglais)
- GRALLA, Preston. *PC Pest Control*, Sebastopol, O'Reilly Media Inc., 2005, 275 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour : 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Logiciel publicitaire (*Adware*)

Qu'est-ce que c'est?

À la télévision, dans les journaux, sur la route, dans les toilettes... La publicité est partout et les ordinateurs n'y font pas exception. Il existe d'ailleurs des logiciels qui se font un devoir de l'afficher sur le plus d'écrans possible : les logiciels publicitaires. Contrairement aux espiogiciels, qui servent également un objectif publicitaire, ils « demandent » habituellement la permission avant de diffuser, afficher, télécharger ou personnaliser de la pub sur un ordinateur, et ils l'obtiennent sans trop de difficulté.

D'un point de vue général, les logiciels publicitaires sont surtout des nuisances, car trop de publicité peut devenir franchement irritant. Toutefois, il s'agit parfois du prix à payer pour utiliser un logiciel ou un service gratuitement. D'un point de vue technologique, ils peuvent causer de sérieux ralentissements, voire des gels.

Plus >>

Comment prévenir et comment guérir?

La plupart des logiciels antiespiogiciels ciblent également les logiciels publicitaires et ils sont en mesure de les éradiquer. La procédure est simple : il est suggéré d'installer au moins deux logiciels antiespiogiciels, de mettre religieusement à jour les signatures d'infection et de scanner un ordinateur une fois par semaine. Pour la tranquillité d'esprit, l'utilisation d'un pare-feu, préalablement bien paramétré, est fortement recommandée.

Gardez toutefois en mémoire que le logiciel publicitaire s'installe sur un ordinateur à la suite du consentement de son utilisateur. Lorsqu'on vous affiche les conditions d'utilisation d'un site et que vous cliquez sur « OK » sans les lire, ou quand vous téléchargez un logiciel gratuit et acceptez la licence d'utilisation sans la consulter, vous donnez votre autorisation. Il est vrai que l'information transmise dans ces conditions et licences peut être difficilement compréhensible. Mais rappelez-vous que tout y est décrit quant à l'utilisation de vos renseignements personnels, de l'envoi de publicité, etc. Si vous les acceptez « à l'aveugle », c'est à vos risques et il se peut que vous receviez de la publicité.

Plus >>

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la securite Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Logiciel publicitaire (*Adware*)

1. Qu'est-ce que c'est?

Il s'agit d'un petit logiciel destiné à diffuser, à afficher et (ou) à télécharger de la publicité sur un ordinateur, qu'elle soit générale ou personnalisée selon certains renseignements recueillis. À l'inverse de son proche cousin, l'espiogiciel, le logiciel publicitaire demande la permission avant de passer à l'action. Et la majorité des internautes acceptent.

<< Retour

2. Comment ça fonctionne?

Le logiciel publicitaire s'infiltre habituellement dans un ordinateur en passant par une application, qu'il s'agisse d'un logiciel, d'un gratuiciel ou d'une application Web. Dès que l'internaute utilise cette application, un ou plusieurs logiciels publicitaires sont installés sur sa machine et cette opération ne s'effectue pas totalement à son insu.

Les concepteurs de logiciels, gratuiciels et applications Web énoncent leurs intentions publicitaires dans la licence d'utilisation ou dans les conditions d'utilisation. Il y a matière à controverse lorsqu'on se penche sur la « clarté » de ces propos, parfois difficilement assimilables ou compréhensibles. Les internautes, désireux d'utiliser les logiciels et services offerts et dans l'impossibilité de saisir les implications « publicitaires » de leur geste, acceptent alors « aveuglément » ces énoncés et subissent les contrecoups publicitaires, sans trop comprendre pourquoi cela se produit.

La controverse est sensiblement la même lorsqu'on observe les moyens de diffusion des logiciels publicitaires, surtout dans les sites Web. En effet, il arrive que des sites soient conçus expressémment pour la propagation de logiciels publicitaires. Dès qu'un internaute y « met le pied », ces parasites peuvent infiltrer son ordinateur sans qu'il s'en aperçoive, par exemple en exploitant une faille du navigateur.

Une fois bien installé, le logiciel publicitaire peut afficher une multitude de publicités diverses. Ou encore, à l'image de l'espiogiciel, il peut enregistrer les activités effectuées sur un ordinateur (en recueillant l'historique de navigation) et utiliser ces données pour présenter de la publicité personnalisée.

CULTURE GÉNÉRALE

Le populaire logiciel de messagerie instantanée Windows Live Messenger (anciennement MSN Messenger) est un gratuiciel. Cependant, son utilisation a un « prix » : il ouvre la porte à toutes sortes de logiciels publicitaires. Leurs activités sont permises par Windows Live Messenger parce qu'elles sont légales et conformes à la réglementation publicitaire en vigueur (exemples de publicité non conforme : la pornographie, la violence, etc.).

Un type de logiciel publicitaire fait d'ailleurs rage sur Windows Live Messenger depuis quelques années : ceux qui envoient automatiquement à une liste de contacts un message peu subtil contenant un hyperlien (exemple : *I lost 10 pounds in a week! Click here to see how I did it.*). Aucune activité de fraude n'est liée à ce message, c'est purement... publicitaire.

De plus, Windows Live Messenger peut recueillir des données personnelles pour présenter de la publicité personnalisée dans un espace réservé à cet effet.

Pour en savoir plus, consultez la Déclaration de confidentialité en ligne de Microsoft, qui régit plusieurs produits de Microsoft, dont Windows Live Messenger.

- Déclaration de confidentialité en ligne de Microsoft
- Résumé des principaux éléments de cette déclaration de confidentialité

C'est la réalité d'Internet. Le réseau est accessible à tous, ce qui inclut les publicitaires aux méthodes douteuses. Les internautes doivent alors apprendre à être vigilants, à être conscients de leurs actes et surtout, de leurs conséquences.

Vous trouvez ça épouvantable? N'oubliez pas que vous donnez votre accord en acceptant la licence d'utilisation ou les conditions d'utilisation pour obtenir un logiciel ou un service gratuitement. De plus, d'un point de vue légal, cette façon de faire pour présenter de la publicité aux internautes est conforme.

Que pouvez-vous donc faire? Utilisez des logiciels de rechange! Vous obtiendrez exactement les mêmes services, le risque publicitaire en moins.

<< Retour

3. Quelles en sont les conséquences?

L'objectif du logiciel publicitaire est de diffuser, afficher ou télécharger de la publicité sur des ordinateurs. Ainsi, la principale conséquence est une exposition publicitaire forte ou légère, selon la

quantité de logiciels publicitaires installés.

Si un intrus venait apposer de la publicité personnalisée sur les murs de votre maison, cela vous agacerait sérieusement. Sur un ordinateur, c'est tout aussi agaçant, sans oublier que ces publicités peuvent considérablement ralentir le fonctionnement d'un ordinateur.

Il ne faut également pas négliger les risques pour la confidentialité des renseignements des internautes. Certains logiciels publicitaires recueillent divers renseignements pour personnaliser leur publicité, ce qui peut compromettre la vie privée des utilisateurs.

<< Retour

4. Comment prévenir?

Plusieurs logiciels sont impliqués dans la protection contre les logiciels publicitaires :
Soit dit en passant, les gratuiciels proposés dans ce site sont exempts de logiciels publicitaires. Développés dans la conformité et servant un objectif d'accessibilité, et non de profit, ils sont offerts gratuitement aux internautes pour favoriser l'accès à des logiciels de qualité.

- Au moins deux logiciels antiespiogiciels dont les signatures d'infection sont à jour;
  - Pensez à scanner votre ordinateur avec chaque antiespiogiciel au moins une fois par semaine.

    ATTENTION :

    Scanner votre ordinateur plusieurs fois par semaine avec chaque antiespiogiciel peut être nécessaire si :
    - Votre ordinateur est ouvert et connecté à Internet durant de longues heures; ou
    - Vous faites beaucoup de téléchargement (en tous genres).
- Un pare-feu correctement paramétré;
- Un logiciel « de ménage », pour nettoyer votre ordinateur des éléments qui pourraient « nourrir » les logiciels publicitaires;
  - Pensez à scanner votre ordinateur et votre base de registre au moins une fois par semaine.
- Une protection antiespiogicielle en temps réel;
- Votre système d'exploitation, il doit être à jour;
- Votre navigateur, il doit être à jour;
- Votre logiciel de courriel (si vous en utilisez un), il doit être à jour;
- Tous les logiciels que vous utilisez pour vos activités ludiques sur Internet. Les logiciels les plus populaires seront davantage ciblés par les logiciels publicitaires, car ils permettent à un publicitaire d'avoir accès à plus de clients potentiels... Optez pour des logiciels de rechange, tout aussi efficaces et moins populaires;

- Votre tête, car la vigilance est de mise! Faites attention de ne pas céder à la tentation du « gratuit » sur Internet...

<< Retour

5. Comment guérir?

Vous êtes infecté par un logiciel publicitaire? Voici ce que vous pouvez faire.
Soit dit en passant, les gratuiciels proposés dans ce site sont exempts de logiciels publicitaires. Développés dans la conformité et servant un objectif d'accessibilité, et non de profit, ils sont offerts gratuitement aux internautes pour favoriser l'accès à des logiciels de qualité.

1. Installez tout de suite un pare-feu, pour éviter que ne problème ne prenne de l'ampleur.
2. Analysez votre ordinateur avec un logiciel antiespiogiciel .
   Supprimez les menaces détectées, s'il y en a.
3. Analysez votre ordinateur avec un deuxième logiciel antiespiogiciel.
   Supprimez les menaces détectées, s'il y en a.
4. Passez un petit coup de balai avec un logiciel « de ménage ».
   Supprimez les résidus détectés.
5. Si malgré toutes ces analyses le logiciel publicitaire subsiste, faites ceci
   a. Redémarrez votre ordinateur en mode sans échec.
   b. Faites une analyse antiespiogicielle (avec un logiciel antiespiogiciel). Supprimez les menaces détectées, s'il y en a.
   c. Redémarrez votre ordinateur en mode Normal.
6. Certains logiciels publicitaires sont plus tenaces alors, s'il est toujours là malgré toutes ces analyses, vous devrez faire un peu de recherche...
   a. Notez le nom du logiciel publicitaire tel qu'il vous est apparu la première fois, lorsqu'un logiciel vous a signalé sa détection.
   b. Allez sur ce site, Commentçamarche.net. Cette communauté informatique offre des forums de discussion où une foule de gens, des professionnels du milieu ou des internautes munis d'une solide expérience dans le domaine, sont prêts à vous aider en tout temps.
   c. Tapez le nom du logiciel publicitaire dans la zone de recherche. N'hésitez pas à poser des questions si vous ne trouvez pas une réponse qui vous convient!

   Un grand sage a un jour dit : « Si ça vous arrive, c'est sûrement déjà arrivé à quelqu'un d'autre... Et cette autre personne a certainement cherché une réponse dans un forum. » ;-)

<< Retour

7. Sources documentaires

- Grand dictionnaire terminologique
- Internet Security Zone.com
- Le Jargon français
- Microsoft (1)
- Microsoft (2)
- Softpedia (anglais)
- Wikipédia (français)
- CHARTON, ÉRIC. *Spywares et virus : Protégez-vous des logiciels escrocs*, coll. « Kit Campus », Paris, CampusPress, 2005, 245 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

Trousse administrateur pirate (*Rootkit*)

Qu'est-ce que c'est?

Le *rootkit*, c'est le magicien des menaces Internet. Il s'agit d'un petit programme, ou d'un ensemble de programmes, permettant de maintenir un accès au coeur d'un système infecté. Bref, comme son nom l'indique, c'est un *kit* utilisé pour conserver un accès *root*[1] (ou accès à la racine du système, en son coeur).

Comment fonctionne-t-il? En suivant trois étapes* :

1. Infiltrer le coeur d'un système;
2. S'y installer confortablement;
3. Camoufler les traces de son intrusion et de ses activités.

Cette dernière étape est cruciale, puisqu'il s'agit d'une particularité propre au *rootkit*. Il arrive en effet à faire « disparaître » toute trace de sa présence (fichiers, processus, clés de registre, autres parasites , etc.) dans le radar des logiciels de sécurité. Ainsi, il peut agir sur une longue période sans être détecté, ce qui rend l'accès *root* disponible très longtemps pour un ou plusieurs pirates. Il peut également camoufler ses activités, déterminées dans sa charge finale. Cette charge finale est en fait la partie exécutable du *rootkit*, celle qui lui permet de causer les dommages pour lesquels il a été programmé.

Plus >>

Comment prévenir et comment guérir?

La suppression des *rootkits* n'est pas des plus aisées. Il existe des logiciels qui se spécialisent dans leur détection et leur éradication, mais il faut bien le choisir, car ils ne sont pas tous simples à utiliser.

Toutefois, pas de panique : de nos jours, les logiciels antivirus offrent des solutions *antirootkit*, efficaces si les signatures d'infection sont à jour. Il existe également des logiciels *antirootkit*. De plus, il est important de mettre régulièrement à jour le système d'exploitation d'un ordinateur pour éviter toute infiltration, d'utiliser un pare-feu et bien sûr, d'être vigilant.

Plus >>

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise a jour . 4 janvier 2011

Ce site a eté conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Trousse administrateur pirate (*Rootkit*)

1. Qu'est-ce que c'est?

Comme il a été mentionné à la page précédente, le *rootkit* est un petit programme, ou un ensemble de programmes, qui permet de maintenir un accès au coeur d'un système infecté, tout en dissimulant toute trace d'infiltration et d'activité. Ces traces peuvent être des fichiers, des processus, des clés de registre, d'autres parasites , des bouts de code, etc. Comme le ferait un magicien, il est en mesure de créer une illusion, celle que « tout va bien », même si en réalité il y a infection.

Non seulement peut-il cacher plusieurs traces, mais il est également en mesure de se dissimuler lui-même, ce qui lui permet d'agir sur une longue période et de causer de lourds dommages. Il peut aussi offrir à un (ou plusieurs) pirate un accès « longue durée » au coeur du système. On peut donc le décrire comme un *kit* pour conserver un accès *root* dans le système infecté[1], qu'il s'agisse d'un ordinateur ou d'un réseau.

<< Retour

2. Comment ça fonctionne?

Maintenant, qu'en est-il de son fonctionnement? Le processus sommaire en trois étapes de la page précédente est un bon résumé, mais il mérite d'être approfondi.

1. Il infiltre un système, qu'il s'agisse d'un ordinateur ou d'un réseau. Pour y arriver, il peut employer différentes techniques:
   a. exploiter une faille;
   b. utiliser un autre parasite comme « vecteur d'infiltration ». Il pourrait par exemple utiliser un cheval de Troie pour assurer sa propagation et son infiltration, ou encore employer un enregistreur de frappe pour acquérir les noms d'utilisateur et mots de passe

nécessaires;

c. employer une attaque ciblée pour « deviner » les mots de passe nécessaires à son infiltration. Par exemple, l'attaque par force brute essaie toutes les combinaisons de caractères possibles (mots simples, association simpliste de chiffres et de lettres) pour finalement obtenir celle qui constitue le mot de passe. Plus le mot de passe est simple, moins il est sécuritaire, car il sera facile à obtenir lors d'une telle attaque.

2. Il s'installe confortablement dans le système infecté. C'est à ce moment qu'il « déclenche » ses activités, ou sa **charge finale**. C'est cette charge finale qui permet au *rootkit* d'obtenir les droits administrateurs et d'exploiter les ressources du système. Selon les intentions du pirate à son origine, elle peut également :
   a. modifier le système en profondeur;
   b. ouvrir une (ou plusieurs) porte dérobée vers le coeur du système et la maintenir ouverte, ce qui permet à un pirate d'en prendre le contrôle;
   c. installer d'autres parasites;
   d. joindre le système à un *botnet*.
3. Il se camoufle et cache toute trace de son intrusion et de ses activités. Cette dissimulation est rendue possible grâce à une ou plusieurs portes dérobées ouvertes par le *rootkit*, qui permettent à un ou plusieurs pirates de venir « bidouiller » au coeur du système. Plus les droits administrateurs obtenus sont élevés dans la hiérarchie, plus ce « bidouillage » gagne en latitude. La corruption de différents fichiers de journalisation (fichiers *log*) empêche également l'enregistrement des activités du *rootkit*. L'objectif est alors de passer inaperçu pour exploiter le système et exécuter sa charge utile le plus longtemps possible.

<< Retour

3. Quelles en sont les conséquences?

Les conséquences varient pour chaque *rootkit*, selon la programmation de leur charge finale. Certains ciblent les données des victimes (fichiers, renseignements personnels, etc.), qu'ils cherchent à usurper afin de procéder ultimement à un vol d'argent ou d'identité. D'autres visent plutôt la prise de contrôle d'un système et l'ampleur des dommages n'aura comme limites que celles de l'esprit humain.

D'autres conséquences peuvent survenir, volontairement ou non, car le camouflage de certains fichiers systèmes pour dissimuler un *rootkit* peut amener des problèmes non prévus. Par exemple, de telles manipulations peuvent créer des failles et affaiblir davantage le système.

CULTURE GÉNÉRALE

> En 2005, la division Music Entertainment de la compagnie Sony BMG avait fait les manchettes, car elle avait procédé à l'installation d'un *rootkit* sur les CD des artistes gérés par Sony BMG. Ce *rootkit* avait pour objectif initial de protéger le contenu des disques vendus contre les copies illégales, mais son « mandat » s'est considérablement élargi :

- Il recueillait des renseignements sur les utilisateurs/acheteurs du CD, à la manière des espiogiciels;
- Il altérait le bon fonctionnement de l'ordinateur, puisqu'il cachait certains fichiers systèmes importants;
- Il aurait amené l'ouverture de failles importantes pouvant être exploitées pour propager d'autres parasites .

On le devine, cette situation a causé bien du tort à Sony BMG, qui s'est toutefois engagée dans plusieurs pays à reprendre les CD infectés et à dédommager les clients.

<< Retour

4. Comment prévenir?

Avec les *rootkits*, rien ne vaut la prévention et voici quelques mesures à appliquer :

- Installer un logiciel antivirus comprenant une solution *antirootkit* et mettre à jour régulièrement les signatures d'infection .
  - Pensez à l'activer en tout temps et à scanner votre ordinateur au moins deux fois par mois.
- Installer un pare-feu et le paramétrer adéquatement.
- Installer un logiciel *antirootkit*, en cas d'infection.
  - Pensez à scanner régulièrement votre ordinateur, une fois par semaine si nécessaire.
- Mettre régulièrement à jour votre système d'exploitation et vos différents logiciels, qu'ils soient liés de près ou de loin à Internet.
  - De près : navigateur, logiciel de courriel,logiciel de messagerie instantanée, logiciel de lecture des documents PDF, lecteur de musique, etc.
  - De loin : suite bureautique, logiciels de graphisme, jeux (s'ils nécessitent des mises à jour), logiciels nécessaires au fonctionnement de certains périphériques (*drivers*), etc.
- Choisir des mots de passe forts et complexes.
- Utilisez votre tête, car la vigilance est de mise!

<< Retour

5. Comment guérir?

Heureusement pour la grande majorité des internautes, de nos jours, la plupart des logiciels antivirus offrent la possibilité de détecter et parfois, de supprimer les *rootkits.* Malheureusement, ils ne l'offrent pas tous. Soit dit en passant, les logiciels antivirus proposés dans ce site comportent une solution *antirootkit.*

Même quand cette protection est offerte, elle n'est pas toujours complète. En effet, certains logiciels

antivirus vont détecter la présence d'un *rootkit*, mais ils ne le supprimeront pas tous. Dans de tels cas, l'utilisation complémentaire d'un logiciel spécialisé dans l'éradication des *rootkits* est importante.

Vous êtes infecté par un *rootkit*? Voici ce que vous pouvez faire pour maximiser vos chances d'éradication :

1. Installez un pare-feu, pour éviter que le problème ne prenne de l'ampleur.
2. Analysez votre ordinateur avec un logiciel antivirus offrant une protection *antirootkit* (comme Avast! ou Antivir). Supprimez les menaces détectées, s'il y en a.
3. Si des menaces sont détectées, mais ne peuvent être supprimées, utilisez un logiciel *antirootkit* (comme Sophos Anti-Rootkit) pour tenter de les supprimer.
4. Si malgré ces analyses le *rootkit* subsiste, faites ceci :
    a. Redémarrez votre ordinateur en mode sans échec.
    b. Faites une analyse avec un logiciel antivirus offrant une protection *antirootkit*. Supprimez les menaces détectées, s'il y en a.
    c. Si des menaces sont détectées, mais ne peuvent être supprimées, utilisez un logiciel *antirootkit* pour les supprimer.
    d. Redémarrez votre ordinateur en mode Normal.
5. Certains *rootkits* sont plus tenaces alors, s'il est toujours là malgré toutes ces analyses, vous devrez faire un peu de recherche... En effet, les *rootkits* se « perfectionnent » au fil des mois, voire chaque semaine, donc en effectuant une recherche de la sorte, vous aurez accès à l'information la plus récente.
    1. Allez sur ce site, Commentçamarche.net. Cette communauté informatique offre des forums de discussion où une foule de gens, des professionnels du milieu ou des internautes munis d'une solide expérience dans le domaine, sont prêts à vous aider en tout temps.
    2. Tapez le mot « *rootkit* » dans la zone de recherche et consultez l'information qu'on vous présentera. N'hésitez pas à poser des questions si vous ne trouvez pas une réponse qui vous convient.

Un grand sage a un jour dit : « Si ça vous arrive, c'est sûrement déjà arrivé à quelqu'un d'autre... Et cette autre personne a certainement cherché une réponse dans un forum. » ;-)

<< Retour

6. Sources documentaires

- Futura-Techno
- Grand dictionnaire terminologique
- Le Jargon français
- Secuser.com
- Wikipédia (français)

- BLOCH, Laurent et Christophe WOLFHUGEL. *Sécurité informatique : Principes et méthodes*, Paris, Groupe Eyrolles, 2006, 261 p.
- GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition,* coll. « microapp », Paris, Micro Application, 2007, 1247 p.
- KONG, Joseph. *Rootkits BSD : Mieux les comprendre pour mieux s'en protéger*, Paris, Campus Press, 2007, 148 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour : 4 janvier 2011

Ce site a eté conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Ver informatique (*Worm*)

Qu'est-ce que c'est?

Le ver informatique ressemble un peu au virus; dans les deux cas, on parle d'un logiciel malveillant qui endommage un système et qui est en mesure de se répliquer...

Mais la ressemblance s'arrête là. Le ver se propage d'un ordinateur à l'autre en passant par les réseaux (comme Internet) puis en exploitant une faille dans un logiciel. Il se plaît alors à circuler dans le système infecté pour l'affaiblir, un peu comme le ferait un ver dans une pomme. Et il n'a pas besoin de programme « hôte » pour assurer sa descendance, il est entièrement autonome.

Plus >>

Comment prévenir et comment guérir?

Les logiciels antivirus sont en mesure de détecter et, dans certains cas, d'éradiquer les vers informatiques, si bien sûr les signatures d'infection sont à jour. Il est également crucial de mettre le système d'exploitation et le navigateur à jour pour se prémunir contre les vers. L'installation et le paramétrage d'un pare-feu viennent couronner cette protection.

Si, malgré tout, votre logiciel antivirus découvre l'un de ces petits lombrics binaires sur votre machine et qu'il n'est pas en mesure de le supprimer, il existe d'autres solutions, décrites à la page suivante.

Les vers sont sournois et peuvent se télécharger sur un ordinateur lors de votre navigation Web, à votre insu. Bien entendu, les sites de confiance sont moins à risque (même s'ils ne sont pas immunisés). Mais lors de vos séances de surf, évitez les sites douteux et potentiellement dangereux, vous serez encore moins à risque!

Plus >>

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises cheminement communication et langages

Université de Sherbrooke 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Ver informatique (*Worm*)

1. Qu'est-ce que c'est?

Il fut un temps où les disques durs des ordinateurs avaient une capacité de 512 Mo, où les jeux vidéo tenaient sur une série de disquettes et où Internet était encore marginal. À cette époque, les virus régnaient en rois et maîtres sur la contrée des menaces informatiques. Bien que toujours « vivants » sur Internet, ils cèdent de plus en plus le terrain à d'autres parasites, dont le ver informatique.

Lorsqu'Internet s'est imposé, les virus ont continué de circuler et d'infecter, mais les pirates se sont vite aperçu que la méthode traditionnelle de propagation des virus (avec l'implication d'un programme « hôte ») n'était pas « optimale ». Ils se sont alors tournés vers les réseaux, comme Internet, et ils ont développé une menace autonome pouvant y circuler aisément : le ver informatique.

Il s'agit d'un petit logiciel qui peut se reproduire, qui circule dans les réseaux (comme Internet) et qui exploite des failles dans des logiciels pour s'infiltrer, infecter et se propager. Il est entièrement autonome dans ses actions et n'a pas besoin de programme « hôte » pour fonctionner. De plus, si on le compare au virus, ses attaques sont plus diversifiées et de plus grande envergure, entre autres en raison de ses « talents » pour infecter un grand nombre d'ordinateurs.

<< Retour

2. Comment ça fonctionne?

Comme il a été mentionné ci-haut, le ver informatique se propage grâce aux réseaux comme Internet, ce qui inclut le Web et le courriel.

Si l'on prend l'exemple d'un ver circulant sur Internet, voici comment l'infection pourrait se produire :

1. Le ver informatique est créé par un pirate, qui le programme selon ses intentions et ses objectifs.
2. Le pirate l'envoie sur Internet
3. Le ver est programmé pour circuler à travers un port précis (par exemple, le port 4331). Quelques jours plus tard, un internaute utilise un logiciel de pair-à-pair qui ouvre le port 4331 pour permettre un téléchargement illégal. Cet internaute, comme plusieurs, ne sait pas que le port 4331 n'est pas sécurisé sur son ordinateur (absence d'un pare-feu correctement paramétré). Et le problème s'accroît si cet ordinateur n'a pas de logiciel antivirus à jour.
4. Résultat : le ver entre par le port 4331 et il exploite une faille de programmation du système d'exploitation pour infiltrer l'ordinateur.

CULTURE GÉNÉRALE

Il existe 65 536 ports qui connectent un ordinateur à Internet... Ça en fait des portes!

<< Retour

3. Quelles en sont les conséquences?

Lorsqu'un ver informatique s'infiltre dans un ordinateur, il peut s'amuser à circuler librement dans sa mémoire et à faire des dommages sur son passage, un peu comme le ferait un ver dans une pomme. Mais cette partie de plaisir n'est réservée qu'au ver, car pour l'internaute, cela signifie un affaiblissement de son système.

Le système infecté devient alors plus vulnérable non seulement aux paralysies et aux plantages, mais aussi à d'autres infections (espionnage, destruction de données, participation à un *botnet*, installation d'autres parasites, etc.).

<< Retour

4. Des exemples

Un exemple? Le ver informatique Blaster (souvent mentionné comme étant un virus) sévissait durant l'été 2003 et il visait les ordinateurs munis d'un système d'exploitation Microsoft Windows 2000 ou XP. Il se propageait par Internet, plus précisément par le port 135, et s'infiltrait en exploitant une faille béante des systèmes d'exploitation ciblés. L'ordinateur infecté devenant alors très instable.

De plus, Blaster avait une signature bien spéciale (qui était d'ailleurs son action principale) : il provoquait le redémarrage de l'ordinateur après un court délai.

CULTURE GÉNÉRALE

Le 29 août 2003, un jeune homme de 18 ans a été arrêté relativement à la création d'une variante virulente et dommageable du ver Blaster. Il a admis sa culpabilité et a été assigné à une sentence de prison de 18 mois. La cybercriminalité, c'est du sérieux!

Il faut souligner que dans un cas d'infection par un ver informatique de la trempe de Blaster, l'internaute est à risque et tous ses contacts le sont également. En effet, le ver peut se reproduire et s'envoyer automatiquement à tous les contacts qu'il croisera... Et l'internaute peu averti n'y verra que du feu.

Un autre exemple? Le virus I Love You, qui a défrayé les manchettes durant l'année 2000, était en réalité un ver informatique. Il se propageait grâce à un fichier en pièce jointe à un courriel. Une fois la pièce jointe activée, le ver pouvait alors se reproduire et s'envoyer automatiquement à toutes les adresses courriel présentes dans le carnet d'adresses Microsoft Outlook du récipiendaire.

Ce fichier joint se présentait comme une lettre d'amour en format texte, mais en réalité il s'agissait d'un petit script (VBS) qui provoquait la destruction des scripts, des pages HTML, des images JPEG et des fichiers MP3. Cependant, c'est surtout sa vitesse de propagation qui a propulsé ce ver au sommet de la « gloire » : 3,1 millions d'ordinateurs infectés en quatre (4) jours seulement. Bien entendu, il a causé des pertes financières de plusieurs milliards de dollars.

Un dernier exemple? Au printemps 2009, le ver **Conficker** a fait parler de lui dans les médias. Avec plus de 10 000 000 d'ordinateurs infectés à son actif (toutes variantes confondues), il se préparait, selon les rumeurs, à déclencher une attaque massive le 1er avril 2009. Ce déploiement n'a pas eu lieu, mais Conficker a tout de même surpris les spécialistes, notamment par son haut niveau de sophistication. Il se propageait par l'intermédiaire des réseaux mal ou non sécurisés, les clés USB infectées et les ordinateurs non protégés. Il ciblait les ordinateurs Windows et les infiltrait en exploitant une faille de ce système d'exploitation.

Une fois dans un système, il en désactivait les mesures de sécurité (notamment en neutralisant Windows Update). Ses variantes pouvaient également :

- bloquer l'accès à certains sites de sécurité;
- déclencher le téléchargement de logiciels malveillants;
- s'associer à certains processus cruciaux de Windows (ce qui compliquait sa détection et son éradication);
- rallier l'ordinateur à un *botnet*;
- installer un faux logiciel de sécurité;
- installer un bot informatique;
- se connecter à un serveur distant pour se mettre à jour (c'est-à-dire changer de variante).

Vous pouvez vérifier si votre ordinateur a été infecté par l'une des variantes de Conficker en visitant cette page Web :

- Conficker Eye Chart (anglais)

<< Retour

5. Comment prévenir?

Il est impératif d'installer deux logiciels importants pour contrer les vers informatiques : un pare-feu et un logiciel antivirus. Le reste se résume à trois mots : mise à jour.

- Mise à jour des signatures d'infection de votre logiciel antivirus;
  - Pensez à l'activer en tout temps et à scanner votre ordinateur au moins deux fois par mois.
- Mise à jour de votre système d'exploitation;
- Mise à jour de votre navigateur;
- Mise à jour de votre logiciel de courriel (si vous en utilisez un).

Et encore une fois, la vigilance est de mise... Pour plus de sécurité, laissez tomber la navigation sur des sites au potentiel d'infection « élevé » (pornographie, fraude, etc.) et les activités tout aussi risquées (téléchargement illégal, utilisation « aveugle » d'un site de réseautage social, etc.).

Voulez-vous savoir si vous êtes à risque? Comme il a été mentionné ci-haut, les vers informatiques infectent un ordinateur en passant par un port. Cliquez sur le lien ci-dessous pour accéder à un scanner de ports en ligne et voyez quelles portes sont ouvertes sur votre système.

- Zebulon.fr : scanneur de ports

<< Retour

6. Comment guérir?

Vous êtes infecté par un ver informatique? Voici ce que vous pouvez faire.

1. Installez tout de suite un pare-feu, pour éviter que ne problème ne prenne de l'ampleur.
2. Si vous avez un logiciel antivirus installé sur votre ordinateur :
   a. Ouvrez votre logiciel antivirus et démarrez une analyse de votre ordinateur sur-le-champ.
   b. Supprimez les menaces détectées.
3. Si vous n'avez pas installé de logiciel antivirus sur votre ordinateur :
   a. Installez Avast! ou Antivir.
   b. Une fois le logiciel installé, ouvrez-le et démarrez une analyse de votre ordinateur.
   c. Supprimez les menaces détectées.
4. Si malgré cette analyse le ver informatique subsiste, faites ceci
   a. Redémarrez votre ordinateur en mode sans échec.
   b. Faites une analyse antivirus (avec un logiciel antivirus). Supprimez les menaces détectées, s'il y en a.
   c. Redémarrez votre ordinateur en mode Normal.

5. Certains vers sont plus tenaces alors, s'il est toujours là malgré toutes ces analyses, vous devrez faire un peu de recherche...
    a. Notez le nom du ver tel qu'il vous est apparu la première fois, lorsqu'un logiciel vous a signalé sa détection.
    b. Allez sur ce site, Commentçamarche.net. Cette communauté informatique offre des forums de discussion où une foule de gens, des professionnels du milieu ou des internautes munis d'une solide expérience dans le domaine, sont prêts à vous aider en tout temps.
    c. Tapez le nom du ver informatique dans la zone de recherche. N'hésitez pas à poser des questions si vous ne trouvez pas une réponse qui vous convient!

Un grand sage a un jour dit : « Si ça vous arrive, c'est sûrement déjà arrivé à quelqu'un d'autre... Et cette autre personne a certainement cherché une réponse dans un forum. » ;-)

<< Retour

7. Sources documentaires

- Assiste.com
- Branchez-vous.com (1)
- Branchez-vous.com (2)
- Grand dictionnaire terminologique
- Le Jargon français
- Secuser.com
- Wikipédia (français)
- Wikipedia (anglais)
- CHARTON, ÉRIC. *Spywares et virus : Protégez-vous des logiciels escrocs*, coll. « Kit Campus », Paris, CampusPress, 2005, 245 p.
- GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition,* coll. « microapp », Paris, Micro Application, 2007, 1247 p.
- GRALLA, Preston. *PC Pest Control*, Sebastopol, O'Reilly Media Inc., 2005, 275 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la securite Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Virus (*Virus*)

Qu'est-ce que c'est?

L'ensemble de la population a déjà attrapé le virus du rhume et connaît bien son « processus » : il se contracte lorsque la victime n'est pas suffisamment prudente, la fait tousser pour assurer sa propagation et l'affaiblit, ou la rend complètement K. O.

À l'image de son homologue biologique, le virus informatique se contracte lorsqu'un utilisateur est peu vigilant, il utilise les ressources de son système pour se reproduire et se propager, tout en le fragilisant ou en le rendant inopérable.

Concrètement, le virus est un petit logiciel malveillant qui, lors de l'infection, se greffe à un programme « hôte ». Ce n'est que lors du déclenchement de ce logiciel que le virus peut passer à l'acte, c'est-à-dire causer des dommages et surtout, se reproduire pour infecter d'autres ordinateurs.

Plus >>

Comment prévenir et comment guérir?

Comme son nom l'indique, le logiciel antivirus demeure une ressource très efficace contre les virus : installez-le, activez-le en tout temps, mettez religieusement à jour vos signatures d'infection et scannez régulièrement votre ordinateur.

Mais ce logiciel antivirus ne protège pas contre tous les dangers, surtout pas de ceux dont l'origine se trouve à 18 pouces derrière l'écran. La mise à jour des signatures d'infection du logiciel antivirus, la vigilance, une attention particulière aux pièces jointes des courriels reçus et l'abandon des téléchargements douteux et illégaux contribuent fortement à votre protection.

Plus >>

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises cheminement communication et langages

Université de Sherbrooke 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Virus (*Virus*)

1. Qu'est-ce que c'est?

Le virus informatique est un petit logiciel, ou simplement d'un extrait de code malicieux, qui est téléchargé à partir d'Internet, d'un courriel, d'un cédérom, d'une clé USB, d'un lecteur MP3, etc. Par la suite, il se greffe habituellement à un programme « hôte » qui, lorsqu'activé, lui permettra de causer les dommages pour lesquels il a été créé et de se reproduire pour infecter d'autres ordinateurs.

On distingue deux composantes dans le virus, communes à tous les types de virus :

1. La charge finale, c'est-à-dire la partie exécutable du virus, celle qui lui permet de faire les dommages pour lesquels il a été programmé; et
2. Le dispositif de reproduction, ce qui lui permet de se propager.

CULTURE GÉNÉRALE

Le virus est la catégorie de menaces Internet la plus connue. De ce fait, selon Wikipédia, on utilise souvent (et abusivement) le mot « virus » pour désigner toutes sortes de logiciels malveillants. Il est alors plus approprié d'utiliser le terme « logiciel malveillant », puisqu'il représente mieux la diversité des parasites Internet actuels.

<< Retour

2. Comment ça fonctionne?

Habituellement, lorsqu'un virus est greffé à un programme « hôte », il attend que ce logiciel « hôte » soit activé. Ce programme peut être un logiciel légitime déjà installé sur l'ordinateur, comme une composante du système d'exploitation, un utilitaire, etc. L'utilisateur floué peut alors activer le virus à tout moment, inconsciemment.

D'autres virus arrivent avec leur propre programme « hôte », auquel ils sont déjà intégrés. Par exemple, un petit jeu gratuit et très mignon offert en téléchargement sur Internet pourrait contenir un virus.

<< Retour

3. Les types de virus et des exemples

À l'image des virus biologiques, les virus informatiques se distinguent selon leur « espèce ». Voici quelques types de virus toujours actifs de nos jours : :

a. ***Le virus programme, ou virus classique***

Ce type de virus colle parfaitement à la définition « standard » du virus informatique. Il se greffe habituellement à un programme « hôte » au moment de l'infection et lorsque l'utilisateur exécute le logiciel compromis, le virus est automatiquement activé. Il peut alors exécuter sa charge finale et se propager avec son dispositif de réplication.

Fait à noter, il arrive que le déploiement d'un tel virus soit préprogrammé pour une date précise, ou encore à la suite d'une action (ou d'une série d'actions) particulière; on parle alors d'une bombe logique jointe à la charge finale du virus.

Un exemple? Entre 1998 et 2002, le virus Tchernobyl a fait trembler le réseau. Il est encore perçu aujourd'hui comme l'une des menaces les plus destructrices dans l'histoire de l'informatique. Sa particularité résidait dans sa période de déclenchement, programmée pour le 26 avril (date anniversaire de la tristement célèbre explosion de la centrale nucléaire de Tchernobyl) grâce à une bombe logique.

À l'arrivée de la date fatidique, il s'activait et sa charge finale, particulièrement destructrice (à l'image de l'explosion) commandait différentes opérations, dont la suppression de fichiers, afin de rendre le système inutilisable.

b. ***Le macrovirus***

Contrairement au virus classique, le macrovirus se lie à un fichier et non à un logiciel, ce lui permet d'infecter autant un PC roulant sous Windows qu'un MacIntosh, ou un PC roulant sous Linux.

Il s'insère habituellement dans les macro-instructions des logiciels (communément appelées les « macros » dans Microsoft Office) qui ont pour but d'automatiser certaines tâches et qui sont souvent rédigées avec le langage VBA de Microsoft. Ainsi caché dans les macros, il est difficilement repérable par les radars des logiciels antivirus, ce qui complexifie sa détection.

Par exemple, un macrovirus pourrait infecter le fichier « Normal.dot ». Ce fichier est le modèle par défaut de l'ensemble des documents créés avec Microsoft Word. En langage clair, cela signifie que chaque document Word est lié au fichier « Normal.dot » (à moins que les paramètres du logiciel aient été volontairement modifiés).

Si ce fichier est infecté, le virus sera activé chaque fois qu'un document Word basé sur le modèle « Normal.dot » sera créé ou ouvert... Le risque est alors élevé, puisque la grande majorité des utilisateurs de Microsoft Word utilisent ce modèle dans leurs documents.

c. ***Le virus du secteur d'amorçage, ou virus de* boot**

Ce type de virus cible les fichiers nécessaires au démarrage du système d'exploitation. Véritable pionnier parmi ses semblables, il n'a pas besoin d'Internet pour circuler; sa propagation est plutôt tributaire des dispositifs externes comme la disquette, le cédérom, le lecteur MP3 ou la clé USB. Si l'ordinateur est démarré à partir d'un dispositif externe infecté, le virus est alors en mesure d'infecter les fichiers de démarrage et de faire planter le système.

À l'époque où les disquettes étaient les principaux véhicules pour faire passer l'information d'un ordinateur à un autre, les virus de *boot* sévissaient, mais plus Internet a gagné en popularité, plus il a perdu en importance. Cependant, on note un retour discret de ce type de virus avec la popularité et la multiplication des clés USB, lecteurs MP3 et autres dispositifs externes de stockage.

ATTENTION :

Vous avez trouvé une clé USB ou un lecteur MP3 abandonné? Faites bien attention... Si vous branchez l'appareil **avant** le démarrage de votre ordinateur, il y a des risques d'infection par un virus de *boot*. Pourquoi? Parce que selon la programmation de votre BIOS (qui vous est probablement totalement inconnue), il se pourrait que votre ordinateur démarre automatiquement à partir de la clé

USB ou du lecteur MP3 infecté et non à partir du disque dur de votre ordinateur.

Les clés USB (ou tout autre dispositif) abandonnées peuvent également être infectées par d'autres types de logiciels malveillants. Les brancher à un ordinateur **avant ou après** le démarrage, sans vérifications préalables, est toujours **risqué**. Pour plus de détails, consultez les Questions + réponses.

d. ***Le virus-ver***

Il s'agit d'un type de virus récent, puisque ses premières apparitions remontent à 2003. Comme un virus programme, il se greffe à un logiciel « hôte ». Comme un ver informatique, il se propage par Internet et exploite les failles des logiciels. Ses actions son non destructrices, mais tout de même ennuyantes, et il poursuit des objectifs de grande envergure comme les refus de service causés par des attaques par saturation.

QUESTION

« Qu'est-ce qu'une attaque par saturation »? Petite explication... Prenons l'exemple d'un site Web. Lorsqu'il subit une attaque par saturation, cela signifie qu'il est tellement sollicité qu'il finit par « planter », un peu comme un professeur qui fige devant un trop grand nombre d'étudiants avec des questions. Ou encore, le plantage peut résulter d'une requête que le site Web n'est pas en mesure de résoudre, comme si le professeur se trouvait devant une question piège l'empêchant de vaquer à ses tâches habituelles.

Soit dit en passant, ce plantage s'appelle également un refus de service.

e. ***Le virus compagnon***

Le virus compagnon ressemble au virus classique, à la différence qu'il ne se greffe pas à un programme « hôte »; il va plutôt en faire une copie conforme infectée et chercher à lui faire prendre le dessus sur l'original.

En quoi cette copie est-elle dangereuse? Prenons l'exemple d'un virus compagnon, téléchargé sur un ordinateur, qui copie l'incomparable jeu « Démineur ». Comme il a été dit plus haut, le virus cherchera à prendre le dessus sur l'original. Ainsi, il ira narguer la base de registre pour lui dire : « Si tu veux démarrer le jeu « Démineur », tu devras faire appel à moi désormais. »

Le résultat? Chaque fois que l'utilisateur démarrera son jeu favori, la copie infectée s'activera, et non l'original. Le virus pourra alors activer sa charge finale et bien sûr, se répliquer.

f. ***Le virus polymorphique***

On peut comparer le virus polymorphique à un espion qui doit changer d'apparence chaque fois qu'il se déplace. Lorsqu'il se reproduit, il modifie sa programmation (c'est-à-dire les séquences d'octets qu'il contient) pour se camoufler. Ainsi, chaque fois qu'il infecte un ordinateur, il a une signature différente, ce qui lui permet d'échapper au radar des logiciels antivirus.

<< Retour

4. Quelles en sont les conséquences?

Lorsqu'un virus s'active, ses dommages dépendent du type de virus, de sa charge finale et des intentions du programmeur qui l'a créé. Le virus peut supprimer des données personnelles ou des fichiers système (virus classique), il peut faire planter l'ordinateur et son système d'exploitation (virus d'amorçage), il peut agir comme un ver informatique et s'amuser avec le courriel (virus-ver)... L'éventail des conséquences est plutôt large.

Toutefois, tous les types de virus ont une conséquence commune : ils nuisent au bon fonctionnement d'un ordinateur. Ils ont également tous un objectif à atteindre, qu'il s'agisse de détruire, paralyser, boguer, saturer, endommager, infiltrer.. ou simplement vous faire peur.

<< Retour

5. Comment prévenir?

Deux éléments de solution existent pour aider les internautes à se protéger contre les virus :

1. La vigilance! Apprenez à reconnaître les signes avant-coureurs :

    a. N'ouvrez **jamais** une pièce jointe à un courriel munie de l'extension .EXE, .BAT, .COM. PIF, .SCR, .CMD, .ZIP, .RAR;

    b. Ne téléchargez pas de fichiers munis de ces extensions à partir d'un site Web dont la source n'est pas fiable, ou à partir d'un logiciel de pair-à-pair. Bref, laissez tomber les téléchargements douteux et (ou) illégaux.

2. Il est également important d'installer :

    a. Un logiciel antivirus, dont les signatures d'infection sont à jour.

        - Pensez à l'activer en tout temps et à scanner votre ordinateur au moins deux fois par mois.

b. Un pare-feu correctement paramétré.

CULTURE GÉNÉRALE

Les virus ne sont plus les vedettes des menaces Internet comme ils l'étaient autrefois. Il existe tout de même des milliers de virus, en plus des variantes développées au fil du temps. Ils ont toutefois tendance à être supplantés par d'autres menaces plus « sexy » aux yeux des pirates, comme les chevaux de Troie, les vers informatiques , etc.

Cependant, cela ne signifie pas qu'ils ne sont plus à l'œuvre. Ils sévissent toujours, mais leur progression est ralentie, ce qui laisse le temps nécessaire aux développeurs de logiciels antivirus pour créer des signatures d'infection et des méthodes d'éradication efficaces.

<< Retour

6. Comment guérir?

Vous êtes infecté par un virus? Voici ce que vous pouvez faire.

1. Installez tout de suite un pare-feu, pour éviter que ne problème ne prenne de l'ampleur.
2. Si vous avez un logiciel antivirus installé sur votre ordinateur :
   a. Ne paniquez pas.
   b. Ouvrez votre logiciel antivirus et démarrez une analyse de votre ordinateur sur-le-champ.
   c. Supprimez les menaces détectées.
3. Si vous n'avez pas installé de logiciel antivirus sur votre ordinateur :
   a. Installez Avast! ou Antivir.
   b. Une fois le logiciel installé, ouvrez-le et démarrez une analyse de votre ordinateur.
   c. Supprimez les menaces détectées.
4. Si malgré cette analyse le virus informatique subsiste, faites ceci
   a. Redémarrez votre ordinateur en mode sans échec.
   b. Faites une analyse antivirus (avec un logiciel antivirus). Supprimez les menaces détectées, s'il y en a.
   c. Redémarrez votre ordinateur en mode Normal.
5. Certains virus sont plus tenaces alors, s'il est toujours là malgré toutes ces analyses, vous devrez faire un peu de recherche...
   a. Notez le nom du virus tel qu'il vous est apparu la première fois, lorsqu'un logiciel vous a signalé sa détection.
   b. Allez sur ce site, Commentçamarche.net. Cette communauté informatique offre des forums de discussion où une foule de gens, des professionnels du milieu ou des internautes munis d'une solide expérience dans le domaine, sont prêts à vous aider en tout temps.

c. Tapez le nom du virus dans la zone de recherche. N'hésitez pas à poser des questions si vous ne trouvez pas une réponse qui vous convient!

Un grand sage a un jour dit : « Si ça vous arrive, c'est sûrement déjà arrivé à quelqu'un d'autre... Et cette autre personne a certainement cherché une réponse dans un forum. » ;-)

<< Retour

7. Sources documentaires

- Assiste.com
- Grand dictionnaire terminologique
- Le Jargon français
- Secuser.com
- Viruslist.com
- Wikipédia (français)
- BLOCH, Laurent et Christophe WOLFHUGEL. *Sécurité informatique : Principes et méthodes*, Paris, Groupe Eyrolles, 2006, 261 p.
- GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition,* coll. « microapp », Paris, Micro Application, 2007, 1247 p.
- GRALLA, Preston. *PC Pest Control*, Sebastopol, O'Reilly Media Inc., 2005, 275 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Canular (*Hoax*)

Qu'est-ce que c'est?

« Soyez millionnaires en un seul clic, sans effort! », « La petite Joséphine a disparu, l'avez-vous vue? » ou « MSN sera payant dès le 1er avril 2011! »... Les canulars font maintenant partie de notre vie Internet. Ce sont habituellement des messages qui véhiculent de la fausse information et qui incitent les destinataires à passer à l'action sous la promesse d'une récompense ou simplement pour manipuler leur bonne foi. Dans certains cas, les conséquences peuvent être graves (par exemple, lorsqu'une trop grande quantité de messages fait planter un réseau), mais habituellement, ils sont plus une perte de temps qu'autre chose.

Plus >>

Comment prévenir?

Pour éviter de tomber dans le piège des canulars, les internautes doivent se conscientiser. Les millions de messages qui transitent chaque jour sur le réseau ne sont pas tous vrais et ils doivent apprendre à repérer les faux. Il existe d'ailleurs des sites spécialisés dans ce repérage, dont HoaxBuster.com et HoaxKiller.fr.

Avant de répondre à l'un de ces courriels importuns ou de le transférer à vos contacts, renseignez-vous et faites les vérifications nécessaires... Après tout, vous ne souhaitez pas être complice d'une distribution de fausses rumeurs!

Plus >>

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Canular (*Hoax*)

1. Qu'est-ce que c'est?

Littéralement parlant, un canular est une blague. Dans un contexte informatique, il s'agit plutôt de fausse information (périmée ou invérifiable) véhiculée sur Internet, par les internautes eux-mêmes, majoritairement par courriel. Le but du canular est de déclencher une émotion spontanée chez l'internaute (joie, désir, pitié, urgence, révolte, curiosité, etc.) pour l'inciter à faire circuler le message, ce qui le rend complice dans cette distribution de fausse information. Un vieil adage disait qu'il ne faut pas croire tout ce qu'on voit à la télé... C'est la même chose sur Internet.

Pourtant, il ne s'agit pas d'un phénomène nouveau; les canulars existaient bien avant l'arrivée d'Internet. On n'a qu'à penser aux chaînes de lettres postales ou encore, aux légendes urbaines.

Peu importe le message véhiculé, les canulars ont tous une ou plusieurs caractéristiques en commun* :

- On essaie de prendre la victime « par les sentiments ».
  - Exemple :
    « Il faut sauver le petit Jesuis Uninconnu! »
- Les faits relatés sont souvent plutôt flous.
  - Exemples :
    « Le petit Jesuis Uninconnu est disparu il y a six mois. » ou
    « Il a été vu la dernière fois en Europe. »
- Les références sont soit inexistantes, soit trop imposantes.
  - Exemple :
    « Ce message vous est envoyé de la part du vice-président Marketing chez Microsoft. »
- On fait des promesses irréalistes, disproportionnées ou impossibles.
  - Exemples :

« Si vous transférez ce message à 15 personnes, vous recevrez un chèque de 1 000 $! »,
« Soyez millionnaire en un seul clic, sans effort! » ou
« Mon ami Jesuis Uninconnu a suivi ces consignes et le lendemain, sa femme est revenue! »

- On répète encore et encore que ce message n'est pas un canular et qu'il est vrai.
  - Exemple :
    « Tout cela est vrai, je vous le jure! Je ne transférerais pas ce message si ce n'était pas vrai! »
- On signale une alerte, surtout pour alarmer les utilisateurs débutants ou ceux qui ne sont pas au courant des faits signalés. Cette situation est particulièrement problématique lorsqu'on fait croire à l'internaute qu'il doit supprimer des fichiers essentiels au bon fonctionnement de son système d'exploitation.
  - Exemples :
    « N'ouvrez pas un courriel en provenance de courriel@jetaieu.com! Il contient un dangereux virus qui effacera tout sur votre disque dur. » ou
    « Le fichier "essentielpourtonordi.exe" est sur votre ordinateur? Supprimez-le, c'est un virus! ».
- Les adresses courriel de toutes les personnes à qui ce message a été envoyé sont visibles (et il y en a souvent beaucoup), car les internautes ne savent pas toujours comment envoyer un message en rendant invisibles les adresses des destinataires. Il s'agit d'ailleurs d'une occasion en or pour les polluposteurs, qui peuvent y piger une foule d'adresses courriel.

Il ne faut toutefois pas confondre les canulars avec les blagues circulant sur Internet : les canulars véhiculent de la fausse information, tandis que les blagues veulent divertir les destinataires avec du texte, des images ou des fichiers téléchargeables (qui peuvent tout de même comporter des risques).

ATTENTION

Faites bien attention aux fichiers téléchargeables en pièces jointes ou à partir d'un hyperlien, il pourrait s'agir de logiciels malveillants... à l'insu de celui ou celle qui l'a envoyé!

Il existe également le *viroax*, une variante unique dont la calligraphie regroupe « canular » et « virus » (au sens large du terme). Ce type de canular incite un internaute à télécharger un fichier, qui est en réalité un logiciel malveillant, en ouvrant une pièce jointe ou en cliquant sur un hyperlien. Pour le convaincre, il peut ajouter que ce fichier est indispensable au bon fonctionnement du système d'exploitation ou d'un autre logiciel (comme le logiciel antivirus, le pare-feu, etc.)

<< Retour

2. Comment ça fonctionne?

À l'origine du canular, il y a une ou plusieurs personnes qui désirent faire une blague douteuse, qui veulent prouver leur importance en faisant circuler un message autour du monde ou encore, qui ont l'intention d'interpeller ou de déranger le plus de gens possible.

Par la suite, cette personne, ou ce groupe, rédige un courriel et y ajoute le plus d'ingrédients possible pour le rendre crédible.

Finalement, le message est envoyé à plusieurs internautes, qui se chargeront de le faire circuler.

<< Retour

3. Le marketing et un exemple

Même si le fonctionnement paraît simple, il a une portée non négligeable. Si le message original est envoyé à 10 personnes et que chacune d'entre elles l'envoie à 10 autres internautes, 100 personnes recevront le message en quelques minutes seulement. Il suffit d'imaginer la portée d'un tel message s'il circule pendant 10 ans.

Cette caractéristique unique du canular a capté d'attention de certaines entreprises, qui ont décidé de l'utiliser pour remplir des objectifs marketing.

Un bon exemple de cette stratégie à l'éthique douteuse est survenu en juin 2008. Avez-vous entendu parler des ondes cellulaires qui peuvent faire éclater des grains de maïs soufflé? Peut-être avez-vous lu cette nouvelle sur un site Web dédié aux nouvelles technologiques, visionné une vidéo sur le Web ou encore reçu un courriel à cet effet?

- Tout un canular! (anglais)

Ce canular a en effet dépassé les limites du courriel en trompant non seulement les internautes, mais également les médias qui se sont empressés de publier la nouvelle sur Internet, au même rythme que les internautes qui transféraient le message à leurs proches. Et il s'agissait bien d'un canular...

Cependant, ce n'était pas un canular comme les autres. C'était un message trompeur particulièrement convaincant (surtout avec les vidéos), propagé dans le cadre d'une campagne de marketing viral et mis en ligne par la société Cardo Systems pour faire la promotion de leurs oreillettes sans fil pour téléphone cellulaire. D'un point de vue marketing, c'était un succès... Mais plusieurs questions éthiques ont fait surface et elles attendent toujours des réponses.

<< Retour

4. Quelles en sont les conséquences?

D'un point de vue social, la conséquence la plus flagrante des canulars est la perte de temps qu'ils engendrent chez les internautes de bonne foi, qui se font un devoir personnel de suivre les consignes du message et de transférer le canular à leurs proches. De plus, certains canulars se spécialisent dans la désinformation, ce qui peut alors porter préjudice à une entreprise, à une société, à une cause, à une famille, à une personne... La crédibilité des vrais courriels d'information peut également en être entachée.

D'un point de vue technique, les canulars envoyés en grand nombre peuvent engorger un réseau (par exemple, celui d'une entreprise) et même le faire planter, ce qui empêche les internautes concernés d'utiliser Internet.

D'un point de vue éthique, les canulars soulèvent plusieurs problématiques, dont celles de l'implication involontaire des internautes dans la propagation de fausse information et le mensonge flagrant qui leur est présenté dans le seul but de les faire agir. Il y a là matière à réflexion.

<< Retour

5. Comment prévenir?

Aucun logiciel ne peut vous protéger contre les canulars. Votre tête est votre meilleure arme. Mais il existe toutefois des outils pour guider votre jugement.

1. Tout d'abord, apprenez à reconnaître les caractéristiques des canulars, mentionnées plus haut.
2. Ensuite, si vous avez des doutes, consultez un site Web se spécialisant dans le référencement des canulars et vérifiez si le message que vous avez reçu en est un. Ces sites sont particulièrement bien documentés; si votre message est un canular, vous le saurez.
    - HoaxKiller
    - HoaxBuster
3. Finalement, si le message est bel et bien d'un canular, évitez d'y répondre ou de le transférer à vos proches. Jetez-le plutôt à la poubelle.

IMPORTANT

Pour éviter les risques associés aux *viroax*, blindez-vous derrière un bon parc-feu et un bon logiciel antivirus.

<< Retour

6. Sources documentaires

- HoaxKiller.fr
- HoaxBuster.com
- Wikipédia (français)
- YouTube - CNN (anglais)
- GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition,* coll. « microapp », Paris, Micro Application, 2007, 1247 p.

<< Retour

Dernière mise à jour : 4 janvier 2011

Ce site a eté conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Hameçonnage (*Phishing*)

Qu'est-ce que c'est?

L'hameçonnage n'est pas un logiciel malveillant, mais bien une technique malveillante permettant à un pirate d'arnaquer ses victimes. L'hameçonnage implique la création d'un courriel convaincant, envoyé massivement, et d'un site Web factice imitant à la perfection l'identité visuelle d'institutions ou d'organisations de confiance (comme une banque, une entreprise, etc.). Sous un faux prétexte, on incite les internautes peu vigilants à « mordre à l'hameçon » et à remettre divers renseignements confidentiels, comme les numéros d'assurance sociale, mots de passe et autres numéros de carte de crédit.

Bref, ce sont la naïveté et la crédulité des internautes qui sont ciblés. S'ils tombent dans le piège, ils sont à risque de subir un vol de données, d'argent ou d'identité.

Alors, pensez-y... Si un inconnu, muni d'un sourire éclatant et prétendant travailler pour une grande institution, frappait à votre porte pour vous soutirer des renseignements confidentiels, vous hésiteriez certainement à les lui remettre... C'est la même chose sur Internet, il faut avoir des doutes tous les courriels qui demandent de l'information, même s'ils sont très convaincants.

Plus >>

Comment prévenir et comment guérir?

Vigilance, vigilance et vigilance, tels sont les trois mots d'ordre pour se protéger contre l'hameçonnage. Il existe également des logiciels se spécialisant dans le repérage des sites factices liés aux courriels d'hameçonnage, mais il faut les percevoir comme des compléments à la vigilance et non des protections complètes en soi. L'emploi d'un logiciel antivirus et d'un pare-feu correctement paramétré est aussi suggéré, en plus de la mise à jour régulière du système d'exploitation et du navigateur.

Il faut savoir qu'aucune banque, aucune organisation financière ni aucune entreprise sur le Web n'envoie de courriels à ses clients pour leur **demander** des renseignements. Ils utilisent les courriels uniquement pour **informer**. Ainsi, si vous recevez un courriel vous demandant de fournir de l'information, il y a de très fortes chances que ce soit une arnaque; jetez-le immédiatement à la poubelle.

Plus >>

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Hameçonnage (*Phishing*)

1. Qu'est-ce que c'est?

L'hameçonnage est une technique d'arnaque visant à usurper l'identité visuelle d'une institution de confiance, puis à l'utiliser pour soutirer des renseignements personnels à des internautes. Sous les couverts d'un faux prétexte, on veut inciter les victimes à remettre d'elles-mêmes de précieux renseignements, sans avoir à les voler. Pour mener à bien cette collecte frauduleuse, la technique exige souvent l'utilisation d'un courriel (l'hameçon) et d'un site Web factice, bien que certains cas d'hameçonnage par téléphone aient été recencés.

Fait à noter, les courriels d'hameçonnage sont habituellement envoyés en masse, un peu comme le sont les pourriels (sauf dans les cas d'attaques par harponnage - ou *spear phishing* - qui ciblent un individu ou un groupe de personnes précises). Et contrairement à ce que plusieurs pourraient croire, ils peuvent être extrêmement convaincants, surtout parce qu'ils imitent à la perfection l'apparence des courriels fiables.

QUESTION

« Quelle est la différence entre les pourriels et les courriels d'hameçonnage? » Excellente question. Dans les deux cas, on parle de sollicitation massive par courriel et il arrive que certains pourriels cherchent à soutirer des renseignements aux internautes. La particularité des courriels d'hameçonnage est qu'ils **imitent** l'apparence de courriels fiables, contrairement aux pourriels qui **créent** leur propre apparence.

L'hameçonnage est basé sur un concept voulant que l'humain soit la plus grosse faille de tout système informatique[1]. Pour arriver à exploiter cette « brèche », bon nombre de pirates n'hésitent pas à faire usage de la fraude psychologique pour inciter les victimes à agir et à ultimement remettre les renseignements recherchés.

Prenons un cas « typique » d'hameçonnage. Un internaute reçoit un courriel d'une banque avec qui il fait affaire. On lui indique que la banque a vécu des difficultés informatiques nécessitant la

désactivation temporaire de son compte. Les problèmes étant maintenant réglés, l'internaute est invité à réactiver son compte en cliquant sur un hyperlien. Dès qu'il clique dessus, il est dirigé vers un formulaire Web sur un site factice identique à celui de l'institution imitée. Puisqu'il est sur un site factice, tous les renseignements inscrits dans ce formulaire tomberont inévitablement entre de mauvaises mains.

Depuis quelques années, l'hameçonnage est devenu payant pour les pirates, ce qui explique en partie leur perfectionnement. L'époque où ces faux courriels contenaient une série de fautes d'orthographe et de syntaxe est révolue (ou presque), tout est maintenant mis en oeuvre pour faire croire aux les internautes qu'ils ont affaire à une organisation ou à une institution qu'ils connaissent et en qui ils ont **confiance**. C'est d'ailleurs pour cette raison que les grands noms sont habituellement utilisés (la Caisse populaire Desjardins, *eBay*, *PayPal*, Facebook, etc.) dans les attaques.

<< Retour

2. Comment ça fonctionne?

Pour comprendre le déroulement d'une attaque par hameçonnage, rien ne vaut un exemple. Prenons celui d'une attaque commise en novembre 2007 et qui ciblait les clients de la Caisse populaire Desjardins*.

Le 15 novembre 2007, un courriel, qui imitait à la perfection l'identité visuelle de la Caisse populaire Desjardins, a été envoyé massivement à une très grande quantité d'internautes.

QUESTION

« À qui était envoyé ce message? » Les pirates derrière cette arnaque ont eu accès à une banque d'adresses courriel recueillies çà et là sur Internet grâce, entre autres, à de petits bots informatiques programmés exclusivement pour trouver ces adresses.

Si vous êtes enclins à laisser votre adresse courriel un peu partout sur le Web (dans des blogues, forums, concours, formulaires en tout genre, etc.), il se peut qu'elle soit repérée par un bot et qu'elle se retrouve, à un moment ou à un autre, dans l'une de ces banques de courriels. Et il est possible qu'un pirate l'utilise pour vous envoyer un courriel d'hameçonnage.

Dans d'autres cas, cette banque d'adresses courriel peut avoir été volée à la suite d'une intrusion dans un serveur (par exemple, si le serveur d'une entreprise a été infiltré à cette fin, tous les employés pourront alors recevoir un courriel d'hameçonnage.).

Le contenu du courriel mentionnait aux clients de Desjardins que leur compte allait arriver à expiration sous peu. Pour remédier à la situation, ils devaient cliquer sur un hyperlien, pour ensuite entrer leurs données bancaires et divers autres renseignements personnels. Dès que l'internaute cliquait sur l'hyperlien en question, il était dirigé vers un faux site d'apparence identique à celui d'AccèsD de Desjardins, mais dont l'adresse URL différait légèrement...

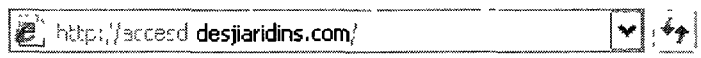
- Adresse URL de la section AccèsD du **site de Desjardins** :

  Mozilla Firefox : 

Internet Explorer : 

- Adresse URL de la section AccèsD du **faux site** :

  Mozilla Firefox : 

  Internet Explorer : 

Avez-vous repéré les différences?

- Tout d'abord, les « vrais » sites bancaires utilisent des pages sécurisées là où des renseignements sont demandés. L'adresse des pages sécurisées commence toujours par « https://... ». L'adresse du faux site ne débutait pas par « https://... ».
- La dernière version de Mozilla Firefox utilise un « entête » spécial dans leur barre d'adresse pour indiquer si le certificat électronique d'un site est valide. Cet entête spécial est affiché sur le vrai site d'AccèsD (en bleu), mais il ne l'est pas sur le faux site. Dans Internet Explorer, un petit cadenas s'affiche à l'extrémité de la barre d'adresse pour signifier que le certificat est valide.
- Ensuite, l'orthographe de « desjardins » est erronée.

Si un internaute tombait dans ce piège, il était guidé à travers une série de pages Web où plusieurs questions lui étaient posées. Le pirate ramassait ainsi un maximum d'information. Enfin, pour tenter de camoufler l'arnaque et la conclure, la victime était redirigée sur le « vrai » site d'AccèsD.

Pour plus de détails, visionnez la vidéo de l'Institut de sécurité de l'information du Québec (ISIQ) expliquant concrètement comment un internaute peut tomber dans un tel piège :

- Cas typique d'hameçonnage

Pour plus d'exemples de courriels d'hameçonnage, consultez le répertoire du site Secuser.com :

- Plus récentes alertes *phishing*

ATTENTION :

Il ne faut pas « chercher des bibittes » là où il n'y en a pas. Les sites qui doivent prouver leur sécurité sont majoritairement ceux où vous devez entrer des renseignements confidentiels (banque, magasin en ligne, concours, etc.).

De plus, ce ne sont pas toutes les pages qui doivent être sécurisées, seulement celles où vous devez inscrire des renseignements.

Alors ne soyez pas inquiet si l'adresse URL de certaines pages informatives de votre site bancaire, ou encore celle de votre site de nouvelles préféré, ne commence pas par « https://... ». Gardez tous vos doutes pour les pages où vous devez **entrer des renseignements confidentiels**.

L'hameçonnage est en constante évolution et les pirates derrière ces arnaques se sont récemment tournés vers les réseaux sociaux. Ces réseaux ont l'habitude d'envoyer des courriels à un membre

lorsqu'un « ami » ou une connaissance désire établir un contact. Certains pirates se sont intéressés à ces courriels pour créer des courriels d'hameçonnage.

Camouflés derrière une fausse identité, ils peuvent créer de faux courriels, identiques à ceux envoyés par les réseaux sociaux, qui vont susciter la **curiosité** des internautes avec un message comme : « Eh! Te souviens-tu de moi? Nous allions à l'école primaire ensemble! » Les internautes seront alors bien tentés de cliquer sur l'hyperlien pour rejoindre le site de réseautage social et entrer en contact avec ladite personne... Pourtant, ils seront souvent redirigés vers des sites factices infectés de chevaux de Troie, espiogiciels et autres parasites à la recherche de renseignements personnels.

Certains courriels d'hameçonnage peuvent même contenir une série de codes malicieux qui téléchargeront automatiquement un ou plusieurs logiciels malveillants dès leur ouverture, ou même s'ils ne sont pas ouverts; le simple fait d'avoir le courriel dans la boîte de réception devient alors risqué.

<< Retour

3. Quelles en sont les conséquences?

Les conséquences liées à l'hameçonnage sont celles qui sont liées au vol de données confidentielles. De la réception massive de pourriels au bombardement publicitaire, en passant par le gel d'un compte bancaire, le vol financier et l'usurpation d'identité, toutes les conséquences occasionnent des pertes pour la victime, qu'il s'agisse de temps ou d'argent.

ATTENTION

Rien de tel que les statistiques pour exposer l'ampleur du problème. Celles recueillies par l'*Anti-Phishing Working Group* révèlent qu'un peu plus de 37 000 cas d'hameçonnage ont été rapportés en juin 2009 seulement.

CULTURE GÉNÉRALE

En 2004, les États-Unis sont allés de l'avant avec l'établissement d'une loi antihameçonnage. Désormais, tout pirate reconnu coupable de fraude bancaire sur Internet (ce qui inclut les attaques par hameçonnage) peut écoper d'une peine de prison de cinq ans.

<< Retour

4. Comment prévenir?

Il existe des logiciels pouvant offrir une protection contre l'hameçonnage, mais ils peuvent vite tomber en désuétude si l'internaute derrière l'écran n'est pas vigilant. L'hameçonnage est une menace qui entre dans la catégorie « humaine », c'est-à-dire qu'elle cible les faiblesses des

internautes au lieu des différentes faiblesses technologiques des systèmes (exploitation d'une faille, attaque par refus de service, etc.) Oui, les logiciels peuvent vous aider, mais la vigilance est votre arme la plus efficace contre cette menace subtile.

Plusieurs logiciels sont impliqués dans la protection contre l'hameçonnage :

- Un logiciel antivirus dont les signatures d'infection sont à jour.
  - Pensez à l'activer en tout temps et à scanner votre ordinateur au moins deux fois par mois.
- Un pare-feu correctement paramétré.
- Un logiciel « de ménage ».
  - Pensez à scanner votre ordinateur et votre base de registre au moins une fois par semaine.
- Votre système d'exploitation, il doit être à jour.
- Votre navigateur, il doit être à jour et en mesure de détecter les sites factices liés à un courriel d'hameçonnage.
- Votre logiciel de courriel (si vous en utilisez un), il doit être à jour et en mesure de repérer les courriels frauduleux.

N'oubliez pas, votre tête reste votre meilleure arme contre l'hameçonnage; faites preuve de vigilance! Et gardez en mémoire les conseils suivants :

- Une banque, ou toute institution financière, n'enverra **jamais** de courriel pour **demander des renseignements**. Les seuls courriels qu'elles pourraient envoyer cherchent à informer et non pas à solliciter de l'information. Alors si vous recevez un courriel d'une banque ou d'une autre institution financière vous demandant de donner des renseignements personnels (en cliquant sur un hyperlien ou directement dans le courriel), il y a de fortes chances que ce soit une arnaque; jetez-le à la poubelle!
- Posez-vous cette question : « Est-ce que j'ai communiqué mon adresse courriel à cette institution? »
- Si vous recevez un courriel douteux contenant un hyperlien, **ne cliquez pas** dessus! Toutefois, vous pouvez glisser votre curseur sur le lien (sans cliquer). L'adresse URL de l'hyperlien devrait apparaître dans la barre d'état, au bas de votre écran. Observez-la attentivement et apprenez à reconnaître les indicateurs de sites factices.
  - Indicateurs de sites factices

Vous avez réussi à ne pas tomber dans le piège? Profitez-en pour signalez la tentative d'hameçonnage à :

- L'organisation canadienne *Phone Busters*; ou
- L'équivalent international, l'*Anti-Phishing Working Group* (anglais).

<< Retour

5. Comment guérir?

Vous êtes tombé dans un piège d'hameçonnage? Voici ce que vous pouvez faire.

1. Ne paniquez pas.
2. Avertissez immédiatement l'institution ou l'organisation concernée, celle utilisée dans le courriel d'hameçonnage (par exemple, votre banque, *PayPal*, etc.). Dites-leur que vous avez été victime d'une attaque par hameçonnage.
    - N'oubliez pas de leur transférer le courriel en question.
    - Profitez-en pour modifier le mot de passe que vous utilisez pour accéder à votre compte sur ce site.
3. Contactez l'une de ces agences canadiennes de renseignements de crédit pour leur signaler que vous êtes à risque de subir une fraude et pour obtenir de l'aide, si nécessaire :
    - TransUnion Canada
    - Equifax Canada
4. Prenez connaissance des ressources mises à votre disposition en cas de vol d'identité.
    - Je protège mon identité sur Internet : vol d'identité
5. Dans certains cas, les courriels d'hameçonnage déclenchent le téléchargement de logiciels malveillants.
    1. Installez un pare-feu, si ce n'est pas déjà fait, et paramétrez-le selon vos besoins.
    2. Analysez votre ordinateur avec un logiciel antivirus.
       Supprimez les menaces détectées, s'il y en a.
    3. Analysez votre ordinateur avec un logiciel antiespiogiciel .
       Supprimez les menaces détectées, s'il y en a.
    4. Analysez votre ordinateur avec un deuxième logiciel antiespiogiciel.
       Supprimez les menaces détectées, s'il y en a.
    5. Passez un petit coup de balai avec un logiciel « de ménage ».
       Supprimez les résidus détectés.

<< Retour

6. Sources documentaires

- Assiste.com
- Grand dictionnaire terminologique
- Je protège mon identité sur Internet
- Phone Busters
- Reasonable Anti-Phishing (anglais)
- Secuser.com
- Wikipédia (français)
- ZDNet - Videos (anglais)
- OCDE. *Document exploratoire sur le vol d'identité en ligne*, 2008, http://www.oecd.org

/dataoecd/51/59/40883671.pdf.

- BEAVER, Kevin. *Combattre les Hackers pour les nuls*, Coll. « Pour les nuls », Paris, Éditions First Interactive, 2004, 423 p.
- CHARTON, ÉRIC. *Spywares et virus : Protégez-vous des logiciels escrocs*, coll. « Kit Campus », Paris, CampusPress, 2005, 245 p.
- GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition,* coll. « microapp », Paris, Micro Application, 2007, 1247 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Pharming

Qu'est-ce que c'est?

L'expression « se jeter dans la gueule du loup » prend tout son sens lorsqu'on parle de *pharming*. Il s'agit d'une technique visant à détourner les adresses URL des sites légitimes pour rediriger automatiquement les internautes vers des sites factices. Et sans surprises, les sites des banques et autres organisations financières sont souvent ciblés.

Comment les internautes peuvent-ils être « attaqués »? Voici un exemple... Lorsqu'un usager tape l'adresse URL du site de sa banque dans son navigateur, il s'attend à être dirigé sur le site de sa banque. S'il subit les contrecoups une attaque par *pharming*, cette adresse est automatiquement détournée, à son insu, et l'envoie vers un faux site d'apparence identique à celui de sa banque. Vous devinez la suite : il inscrit différents renseignements et ce sont les pirates qui les recueillent.

Bien que cette menace ressemble à l'hameçonnage, elle diffère sur un point : aucun courriel n'est impliqué pour mener l'internaute sur un site factice; c'est le détournement de l'adresse URL qui s'en charge.

Plus >>

Comment prévenir et comment guérir?

Pour éviter les attaques par *pharming*, rien ne vaut la vigilance. Vous devez prendre l'habitude de jeter un coup d'oeil aux adresses des pages où vous devez inscrire des renseignements confidentiels (sur le site d'une banque, d'un commerce en ligne, etc.). Assurez-vous d'abord que cette adresse est exacte et qu'elle ne comprend aucun indicateur de site factice. Ensuite, vérifiez si la page est sécurisée, auquel cas son adresse devrait commencer par « **https://...** ». Ces simples gestes pourraient vous éviter bien des problèmes.

- Indicateurs de sites factices

Il existe également des logiciels permettant de repérer les sites factices, mais la prudence demeure le meilleur bouclier. L'emploi d'un logiciel antivirus et au moins deux logiciels antiespiogiciels dont les signatures d'infection sont à jour, en plus d'un pare-feu correctement paramétré, est très important, en plus de la mise à jour **régulière** du système d'exploitation et du navigateur.

Plus >>

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Pharming

1. Qu'est-ce que c'est?

De nos jours, la plupart des gens ont déjà entendu parler de l'hameçonnage (*phishing*), que ce soit par des personnes proches, les médias ou en raison d'une expérience personnelle. Cependant, l'hameçonnage n'est pas la seule menace dans sa catégorie. Parmi ses proches « cousins », on trouve entre autres le *pharming*, une menace méconnue et bien plus dommageable, selon certains spécialistes dans le domaine.

On pourrait décrire le *pharming* comme une technique d'attaque visant à tromper les internautes (d'où la ressemblance avec l'hameçonnage) en détournant les adresses URL des sites Web qu'ils visitent (d'où la différence).

QUESTION

« Mais quel est l'intérêt de détourner une adresse URL? » La réponse à cette question est simple : pour faire de l'argent. Imaginez le scénario suivant :

1. Un pirate repère une banque connue et populaire (Banquefictive.com) dont l'adresse URL est http://www.banquefictive.com. Il décide de l'utiliser pour lancer son attaque.
2. Par la suite, il observe son site Web et s'affaire à en créer un autre parfaitement identique.
3. Finalement, il effectue une attaque par *pharming* pour détourner l'adresse http://www.banquefictive.com vers le faux site qu'il vient de créer. Chaque fois qu'un internaute inscrira l'adresse URL de cette banque dans son navigateur, il sera automatiquement redirigé vers le faux site.
4. Vous devinez la suite... Les clients internautes de Banquefictive.com risquent d'entrer tous leurs renseignements personnels et bancaires sur... un site géré par un pirate.

CULTURE GÉNÉRALE

D'où vient le terme « *pharming* »? Il s'agit d'un dérivé du mot *farm*, utilisé dans le contexte d'un *server farm* (grappe de serveurs), qui est un ensemble de serveurs connectés entre eux pour subvenir à des besoins supérieurs à ce que peut assurer un seul serveur.

<< Retour

2. Comment ça fonctionne?

Le scénario ci-dessus évoque bien le fonctionnement « traditionnel » d'une attaque par *pharming*, mais il mérite d'être approfondi. Comment un pirate arrive-t-il à détourner une adresse URL? Tout commence avec une adresse IP...

Absolument tout ce qui est connecté au réseau Internet possède une adresse IP, une série de quatre segments de chiffres (par exemple, 192.168.0.1) représentant des bits (plus précisément, 32 bits). Chaque adresse IP est un identifiant, que ce soit pour l'ordinateur d'un internaute ou pour un serveur, qui peut d'ailleurs contenir des sites Web. On pourrait comparer les adresses IP à des numéros de téléphone; dans les deux cas, il s'agit d'une série de chiffres liée à une entité.

CULTURE GÉNÉRALE

On peut ultimement accéder à un site Web en entrant, dans la barre d'adresse du navigateur, l'adresse IP correspondant à l'ensemble d'ordinateurs (serveur) qui lui correspondent.

Lorsque les sites Web et les ordinateurs connectés à Internet communiquent entre eux, ils utilisent leurs adresses IP, car ils ne parlent que le numérique. Toutefois, pour les internautes, communiquer sur Internet en emloyant les adresses IP n'est pas chose simple. Les humains ne les retiennent pas facilement, raison pour laquelle elles sont converties en une série de caractères alphanumériques qu'on appelle un nom de domaine. L'adresse URL **http://www.usherbrooke.ca** est bien plus simple à identifier et à saisir que **http://132.210.0.1**, vous ne trouvez pas?

Cependant, la conversion d'une adresse IP en nom de domaine ne se fait pas par magie. Pour y arriver, l'aide du DNS est indispensable. Le DNS, c'est comme un bottin téléphonique. Le bottin sert à établir un lien entre une personne et un numéro de téléphone; le DNS, quant à lui, sert à établir une correspondance entre un nom de domaine et une adresse IP. Ainsi, lorsqu'un internaute tape une adresse URL (par exemple, http://www.usherbrooke.ca), le DNS se charge de convertir le nom de domaine en adresse IP (par exemple, http://132.210.0.1) pour le diriger vers le site demandé.

Le *pharming* est une menace qui cible directement ce DNS, cherchant à le corrompre pour qu'il redirige un nom de domaine conforme vers une adresse IP illégitime, celle du faux site. Et les internautes n'y voient que du feu, car tout ce qu'ils font, c'est ouvrir leur navigateur et taper une adresse URL...

IMPORTANT

Il faut savoir que le DNS est un système et il implique deux choses : les serveurs DNS (côté serveur... c'est-à-dire du côté d'Internet) et le cache DNS (côté client... c'est-à-dire de votre côté, dans votre ordinateur).

Soit dit en passant, les serveurs DNS peuvent également posséder un cache DNS. Toutefois, toute mention « cache DNS » dans ce site fait référence au cache DNS du côté client.

Pour en savoir plus, consultez la fiche Fonctionnement du DNS.

Le DNS peut être corrompu de différentes manières :

- En manipulant le cache DNS dans l'ordinateur d'un internaute (ou ordinateur client)

  On peut comparer ce cache DNS à un aide-mémoire; lorsqu'un internaute visite un site Web, la conversion du nom de domaine en adresse IP, effectuée par le serveur DNS, est gardée en mémoire dans son ordinateur pour accélérer le processus lors de la prochaine visite.

  Certains parasites, comme un virus ou un cheval de Troie, peuvent s'infiltrer dans l'ordinateur d'un internaute pour aller corrompre le cache DNS. Bien entendu, ces parasites sont conçus pour cibler certaines adresses URL précises (comme celles des banques) dans le cache DNS et dès que l'internaute tapera l'une d'entre elles, il sera redirigé vers un site factice.

- En manipulant le serveur DNS dans un serveur ciblé (du fournisseur d'accès à Internet (FAI), ou encore d'un haut serveur de noms de domaine)

  Le serveur DNS, c'est celui qui s'occupe de convertir une adresse IP en nom de domaine, et vice versa. Mais, il ne fait pas cela tout seul; il bénéficie de l'aide de tout un système.

  Tous les serveurs connectés à Internet possèdent un serveur DNS. Par exemple, tous les fournisseurs d'accès à Internet en ont un pour assurer la navigation de leurs clients. Ces serveurs DNS « se rapportent » à d'autres serveurs DNS haut placés, tout ça pour être en mesure de répondre aux requêtes des internautes. Ils respectent tous une hiérarchie bien précise et au sommet de l'organigramme, se trouve le serveur racine du DNS.

  Pour en savoir plus à ce propos, consultez la fiche Fonctionnement du DNS.

  Il s'agit d'un système bien organisé... et complexe! Ce que l'on constate, c'est que plus le serveur DNS attaqué est haut dans la hiérarchie, plus l'ampleur des dommages est importante.

  Lorsqu'un pirate réussit à infiltrer un serveur DNS (peu importe son niveau) en raison d'une vulnérabilité, il peut y ajouter une instruction (qu'on appelle aussi une clé) disant, par exemple :

  « Lorsqu'un internaute tapera l'adresse http://www.banquefictive.com, ne l'envoie pas à l'adresse IP légitime http://192.168.0.1, envoie-le plutôt à l'adresse IP de mon faux site

http://207.168.0.1. »

Ce n'est donc pas qu'un seul internaute qui sera touché par cette attaque, ce seront tous les internautes qui taperont l'adresse http://www.banquefictive.com, jusqu'à ce que l'attaque soit détectée et résorbée.

Voulez-vous savoir si votre ordinateur est vulnérable? Visitez le site de Dan Kaminsky, qui met à votre disposition un *DNS Checker*, et vérifiez si le serveur DNS avec lequel vous faites affaire est en difficulté :

- DoxPara Research (anglais)

CULTURE GÉNÉRALE

Le 8 juillet 2008, Dan Kaminsky a découvert une importante faille dans le système DNS côté serveur. Cette faille n'était pas ordinaire... Elle ne se trouvait ni dans un logiciel, ni dans un ordinateur précis, elle était bien haut dans la hiérarchie du système DNS! L'ensemble de la communauté internaute était à risque.

Étant donné l'importance de cette faille, pour une première fois dans l'histoire d'Internet, tous les géants de l'informatique (dont Microsoft, Sun Microsystems et Cisco) ont allié leurs forces pour développer des correctifs et les distribuer à leurs clients respectifs.

<< Retour

3. Quelles en sont les conséquences?

Le *pharming* est une menace axée sur le profit; les pirates qui la mettent en œuvre désirent la rendre la plus rentable possible. Ainsi, si vous êtes victime d'une attaque par *pharming*, c'est parce que l'adresse URL d'une institution que vous fréquentez (financière ou autres) ou d'un service que vous utilisez a été détournée vers un site factice.

Bref, les conséquences sont celles liées au vol de données bancaires ou confidentielles : vol d'argent, utilisation du compte au profit du pirate, vol d'identité, etc.

< Retour

4. Comment prévenir?

Pour bien vous protéger contre le *pharming*, vous **devez** allier précautions logicielles et précautions humaines.

En ce qui concerne les protections logicielles, voici ce qui est essentiel :

- Utiliser un logiciel antivirus dont les signatures d'infection sont à jour.
  - Pensez à l'activer en tout temps et à scanner votre ordinateur au moins deux fois par mois.
- Utiliser un pare-feu correctement paramétré.
- Utiliser deux logiciels antiespiogiciels dont les signatures d'infection sont à jour;
  - Pensez à scanner votre ordinateur avec chaque antiespiogiciel au moins une fois par semaine.

  ATTENTION :

  Scanner votre ordinateur plusieurs fois par semaine avec chaque antiespiogiciel peut être nécessaire si :
  - Votre ordinateur est ouvert et connecté à Internet durant de longues heures; ou
  - Vous faites beaucoup de téléchargement (en tous genres).
- Mettre régulièrement à jour le système d'exploitation, le navigateur et le logiciel de courriel (si vous en utilisez un).

Toutefois, gardez en mémoire que tous les logiciels du monde ne suffisent pas à vous protéger. Votre meilleure arme est votre vigilance.

- Lorsque vous accédez à un site où vous devez entrer des renseignements confidentiels (une institution financière, un site de commerce en ligne, un service de courriel comme Hotmail, etc.), assurez-vous que l'adresse de la page où vous devez entrer ces renseignements ne comporte aucun indicateur de sites factices.
  - Indicateur de sites factices
- Portez une attention particulière aux certificats électroniques. Ces certificats sont émis par des autorités de certification et servent à lier les entités électroniques (comme un site Web) à des entités physiques (comme un serveur). Les sites de confiance consentent à être identifiés alors, ils affichent leur certificat électronique.

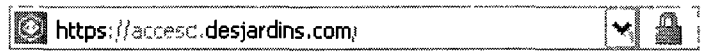
  Cependant, si un site n'est pas de confiance, il peut y avoir des problèmes avec son certificat électronique. Dans un cas de *pharming*, ces problèmes peuvent être :

  1. L'autorité de certification n'est pas reconnue;
  2. Le nom du site n'est pas le même que celui qui est inscrit sur le certificat électronique.

  Chaque navigateur possède une fonctionnalité pour indiquer aux internautes si le certificat du site qu'ils visitent est validé :

  - Certificat valide :

    Mozilla Firefox : 

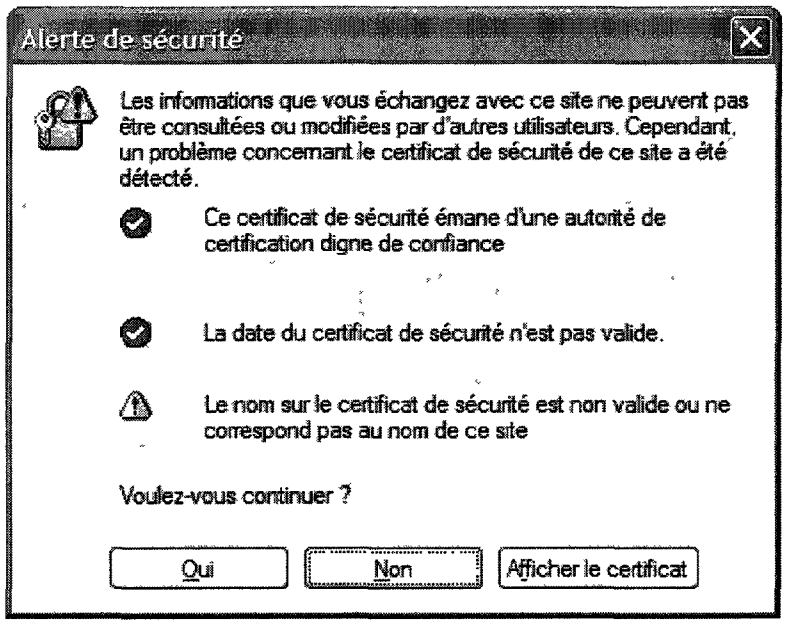
Internet Explorer : 

- Certificat non validé :

Mozilla Firefox : 

Internet Explorer : 

Ou encore, une boîte de dialogue semblable à celle-ci peut apparaître.



Si elle n'apparaît pas, c'est que vous êtes sur un site de confiance. Si elle apparaît, c'est qu'il y a peut-être un problème. À moins d'être sûr à **110 %** que vous êtes sur un site de confiance, cliquez sur « Non ».

<< Retour

5. Comment guérir?

Vous savez que vous avez subi une attaque par *pharming*? Voici ce que vous pouvez faire.

1. Ne paniquez pas.
2. Si vous vous souvenez de l'institution ou l'organisation imitée (banque, commerce en ligne, etc.), avertissez-la. Profitez-en pour changer le mot de passe que vous utilisez pour accéder à votre compte sur ce site.
3. Contactez l'une de ces agences canadiennes de renseignements de crédit pour leur signaler que vous êtes à risque de subir une fraude et pour obtenir de l'aide, si nécessaire :
   - TransUnion Canada

- Equifax Canada

4. Prenez connaissance des ressources mises à votre disposition en cas de vol d'identité.
    - Je protège mon identité sur Internet : vol d'identité

<< Retour

6. Sources documentaires

- Assiste.com
- DoxPara Research (anglais)
- Internet Systems Consortium Inc. (anglais)
- Je protège mon identité sur Internet
- Le Jargon français
- Radio-Canada
- Secuser.com
- Webmaster Hub
- Who.is (anglais)
- Wikipédia (français)
- Wikipedia (anglais)
- ZDNet - Videos (anglais)
- GOMEZ URBINA, Alexandre. *Hacking interdit, 2e édition,* coll. « microapp », Paris, Micro Application, 2007, 1247 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Pourriel (*Spam*)

Qu'est-ce que c'est?

« Des médicaments pas chers! », « Voici LA pilule pour guérir tous vos maux! », « Le logiciel que vous voulez pour 0 $! », tels sont des sujets de pourriels que vous pourriez recevoir. Bien entendu, il s'agit d'une méthode plutôt envahissante pour coller de la publicité sur des écrans d'ordinateur et ils sont souvent jetés à la poubelle.

Mais s'ils sont presque toujours jetés, pourquoi en reçoit-on encore? Parce que le pollupostage est une technique publicitaire facile et à faible risque pour les annonceurs, car elle leur permet de cacher leur identité. L'objectif derrière acte désormais illégal et bien sûr, exempt d'éthique, est d'envoyer un nombre maximal de pourriels en espérant qu'une petite quantité d'internautes y répondent. Par exemple, dans le cas d'un pourriel envoyé à 2 millions d'internautes, si seulement 1 % d'entre eux répondent au message, cela représente tout de même 20 000 clients potentiels.

Les pourriels publicitaires sont les pus fréquents et les plus connus, mais ceux ayant des objectifs malveillants ou irritants, et aucunement publicitaires, existent également.

Plus >>

Comment prévenir et comment guérir?

Si vous recevez des pourriels, c'est parce qu'un polluposteur a repéré votre adresse courriel quelque part sur Internet (sur un forum, dans une séance de clavardage, sur un site Web, etc.). Pour la repérer de la sorte, il a pu utiliser, entre autres, un petit bot informatique dont l'unique tâche est de trouver des adresses courriel et de les enregistrer dans une banque de données.

Vous pouvez utiliser un filtre antipourriel qui se chargera d'analyser les messages entrants et de neutraliser ceux qui présentent des caractéristiques des pourriels. Mais la meilleure façon de les éviter est encore de ne pas les recevoir. Limitez la diffusion de votre adresse courriel « principale » et créez une adresse spéciale réservée aux activités ludiques sur Internet... et profitez-en pour observer le bombardement de pourriels qui résultera de sa diffusion!

Pensez également à protéger votre ordinateur avec une série de logiciels de sécurité dont un logiciel antivirus et au moins deux logiciels antiespiogiciels, dont les signatures d'infection sont à jour, et un pare-feu correctement paramétré. N'oubliez pas aussi de mettre à jour le système d'exploitation de votre ordinateur.

Plus >>

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

Pourriel (*Spam*)

1. Qu'est-ce que c'est?

Le mot pourriel est une fusion des termes « poubelle » et « courriel ». Parfois on l'appelle polluriel ou *spam*, mais peu importe son nom, il s'agit toujours de la même chose : un message non sollicité envoyé massivement et destiné à la poubelle.

Bien que la majorité des pourriels soient envoyés à des fins **publicitaires**, il existe aussi des pourriels **malveillants** (qui déclenchent le téléchargement de logiciels malveillants) ou **irritants** (qui diffusent et martèlent des idées, opinions et autres polémiques).

Les internautes sont conscients de l'existence des pourriels envoyés par courriel, puisqu'il s'agit là du mode d'expédition le plus utilisé. Toutefois, les polluposteurs ne se limitent pas qu'au courriel, ils utilisent également :

- les forums de discussion;
- les fenêtres de conversation d'un logiciel de messagerie instantanée;
- les résultats des moteurs de recherche;
- les blogues;
- les wikis;
- ... et même les téléphones employant la technologie voix sur réseau IP.

Les utilisateurs savent comment supprimer un pourriel reçu dans un courriel, par messagerie instantanée, ou même dans un blogue personnel. Cependant, lorsqu'ils sont confrontés aux pourriels diffusés dans les moteurs de recherche ou dans les forums de discussion, ils sont sans moyens. Pour cette raison, toute la communauté Internet doit être sensibilisée à la réalité du pourriel et à l'importance des mesures de sécurité, ce qui implique à la fois les internautes, les webmestres et les autres travailleurs du Web.

<< Retour

2. Comment ça fonctionne?

Il existe différents types de pourriel et plusieurs canaux de diffusion, tel qu'expliqué au point précédent. Cependant, puisque les pourriels publicitaires envoyés par courriel sont les plus connus, ils seront utilisés pour décrire le fonctionnement de cette menace.

Prenons un exemple fictif, mais tout de même « typique », d'un envoi de pourriel par courriel.

À l'origine, il y a souvent un polluposteur qui cherche à faire de l'argent. Grâce à ses « talents » de pirate, il a réussi à créer son propre *botnet* contenant des centaines, voire des milliers, d'ordinateurs zombies. Le polluposteur a choisi d'utiliser un *botnet* afin de pouvoir se cacher derrière son armée de zombies, sans risquer d'être repéré.

Ses aptitudes lui ont aussi permis de bâtir une liste d'adresses courriel. Il existe différentes manières de récolter des adresses de la sorte, dont la programmation d'un bot informatique qui circule sur différents sites, des forums de discussion, des sites de réseautage social, voire dans les logiciels de messagerie instantanée, à la recherche d'adresses courriel. L'objectif est de bâtir une liste suffisamment volumineuse pour que l'envoi de pourriels soit rentable. Certaines listes peuvent comporter des milliers, voire des dizaines ou des centaines de milliers d'adresses.

Le polluposteur présente ensuite son *botnet* et sa liste d'adresses courriel à différentes « entreprises » potentiellement intéressées à l'utiliser pour diffuser leur publicité.

Une de ces entreprises manifeste de l'intérêt, entre en contact avec le polluposteur et après négociations, elle lui remet un certain montant d'argent. Par la suite, l'entreprise rédige un courriel publicitaire et le remet au polluposteur, qui se chargera de l'envoi massif.

Le polluposteur passe finalement à l'acte et envoie le pourriel à toutes les adresses qu'il possède dans sa liste. Cet envoi requiert beaucoup bande passante, raison pour laquelle les ordinateurs zombies du *botnet* deviennent particulièrement utiles. Le polluposteur leur « vole » leur puissance pour obtenir la « superpuissance » dont il a besoin pour faire son envoi massif. Dès l'envoi est terminé, il ferme le serveur qui gérait le *botnet* pour camoufler toutes les traces de ses actes.

CULTURE GÉNÉRALE

Aux États-Unis, l'envoi massif de pourriels est illégal en raison de la loi antipourriel CAN-SPAM, en vigueur depuis le 16 décembre 2003. Et les peines peuvent être sévères! À la fin du mois de juillet 2008, l'un des dix plus grands polluposteurs du monde (selon Microsoft) a été condamné à près de 4 ans d'emprisonnement pour avoir fait des envois massifs de pourriels.

En ce qui concerne les pourriels malveillants, il est important de souligner qu'ils sont moins fréquents que ses homologues publicitaires. Ils peuvent être distribués de la même manière que ces derniers, même si leur objectif n'a rien de publicitaire. Leur particularité est qu'ils contiennent soit un fichier risqué en pièce jointe, soit un hyperlien qui, lorsque cliqué, déclenchera le téléchargement de logiciels malveillants.

QUESTION

« Quelle est la différence entre les pourriels et les courriels d'hameçonnage? » Excellente question.

Dans les deux cas, on parle de sollicitation massive par courriel et il arrive que certains pourriels cherchent à soutirer des renseignements aux internautes. La particularité des courriels d'hameçonnage est qu'ils **imitent** l'apparence de courriels fiables, contrairement aux pourriels qui **créent** leur propre apparence.

Les pourriels irritants, quant à eux, ressemblent davantage aux pourriels publicitaires, sauf qu'ils sont moins fréquents et que leur message est davantage axé sur une « nouvelle » (rumeur, idée, idéologie, polémique, etc.) que sur de la publicité.

IMPORTANT

Il ne faut pas confondre les pourriels et les envois publicitaires conformes. Les pourriels sont envoyés à des individus qui n'ont jamais consenti à recevoir une telle publicité.

Les courriels publicitaires sont envoyés aux internautes qui ont donné leur consentement (par une case à cocher dans un formulaire de concours, l'inscription à un service en ligne, etc.), même si ce consentement est parfois subtil et facile à oublier.

<< Retour

3. Quelles en sont les conséquences?

La conséquence la plus flagrante de la réception d'un grand nombre de pourriels publicitaires ou irritants est la perte de temps associée à leur suppression. De plus, les envois de pourriels sont parfois si importants qu'ils peuvent engorger les réseaux et les faire planter, ce qui peut entraîner la perte temporaire d'une connexion Internet.

Les conséquences s'aggravent lorsqu'un internaute est victime d'un pourriel malveillant. Ce type de pourriel incite les victimes à télécharger une pièce jointe infectée ou à cliquer sur un hyperlien, ce qui déclenchera le téléchargement de logiciels malveillants (en le menant sur une page Web infestée, par l'activation d'un script malicieux, etc.). Les internautes pris au piège sont alors à risque de subir toutes les conséquences des logiciels malveillants installés.

<< Retour

4. Comment prévenir?

Les internautes peuvent se prémunir contre les pourriels par courriel en employant un filtre antipourriel. Cette fonctionnalité cherche des mots clés que l'on trouve habituellement dans les pourriels. Dès que l'un de ces mots est détecté dans le titre ou dans le corps d'un message, le courriel en question est soit supprimé, soit mis en quarantaine. Les services de courriel gratuits (comme Gmail ou Hotmail), de même que certains logiciels de courriel (comme Mozilla Thunderbird ou Microsoft Outlook) offrent un tel filtre.

Pour se protéger contre les pourriels envoyés par messagerie instantanée, les internautes ne doivent jamais cliquer sur l'hyperlien contenu dans ces messages. La même règle s'applique aux pourriels malveillants.

Les webmestres et autres programmeurs du Web doivent également se sensibiliser à la réalité des pourriels en limitant, au meilleur de leurs capacités, les erreurs de programmation pouvant mener à l'ouverture d'une faille. En effet, un polluposteur pourrait l'exploiter pour afficher de la publicité sur le site attaqué.

Peu importe le type de pourriel, une règle d'or demeure : il faut être **vigilant**. Il est important de limiter au maximum la diffusion de son adresse courriel, pour éviter qu'elle ne soit repérée par un polluposteur puis ajoutée à sa liste d'envoi. Ces derniers peuvent récolter des adresses avec différents moyens et à différents « endroits » (sites de réseautage social, forums de discussion, sites Web en tous genres, logiciels de messagerie instantanée, etc.). La vigilance est donc de mise partout.

QUESTION

« C'est bien beau tout ça, mais je ne tiens pas à me priver sur Internet... » Il est possible de combiner vigilance et divertissement sur le Web. Cela demande un peu de gestion, mais c'est possible.

Une adresse courriel, ce n'est pas comme une adresse postale, vous pouvez en avoir plusieurs. Grâce à des services courriel gratuits comme Hotmail, créez une adresse courriel réservée à vos activités ludiques sur Internet. Vous aurez certes à gérer plus d'un compte courriel, mais de cette manière, la diffusion de votre adresse courriel « principale » sera limitée au maximum et en plus, vous pourrez observer la quantité de pourriels reçus à votre adresse courriel dédiée, sans aucune crise de jurons.

IMPORTANT

Au moment de la création d'une adresse courriel, il est important de choisir des mots ou des chiffres qui ne divulguent aucun renseignement confidentiel (nom, prénom, âge, date de naissance, emploi, etc.). Optez pour un surnom vague, ou pour une série de mots et (ou) de chiffres qui auront du sens pour vous et vos proches, mais pas pour les polluposteurs.

Exemples : je_me_marre_sur_internet@hotmail.com ou boiteverte299@hotmail.com

De plus, soyez proactifs et protégez votre ordinateur des les contrecoups des pourriels avec :

- Un logiciel antivirus dont les signatures d'infection sont à jour;
  - Pensez à l'activer en tout temps et à scanner votre ordinateur au moins deux fois par mois.
- Au moins deux logiciels antiespiogiciels dont les signatures d'infection sont à jour;
  - Pensez à scanner votre ordinateur avec chaque antiespiogiciel au moins une fois par semaine.

ATTENTION :

Scanner votre ordinateur plusieurs fois par semaine avec chaque

antiespiogiciel peut être nécessaire si :

- Votre ordinateur est ouvert et connecté à Internet durant de longues heures; ou
- Vous faites beaucoup de téléchargement (en tous genres).

- Un pare-feu correctement paramétré;
- Une protection antiespiogicielle en temps réel;
- Un logiciel « de ménage », pour nettoyer votre ordinateur de différents éléments parasites;
  - Pensez à scanner votre ordinateur et votre base de registre au moins une fois par semaine.
- Votre système d'exploitation, il doit être à jour;
- Votre navigateur, il doit être à jour;
- Votre logiciel de courriel (si vous en utilisez un), il doit être à jour;
- Votre tête, car la vigilance est de mise!

De plus, n'oubliez pas de **gérer efficacement votre adresse courriel**.

- Si vous utilisez un service de courriel gratuit sur Internet, assurez-vous qu'il offre un bon filtre antipourriel. Voici quelques services gratuits qui offrent des filtres efficaces :
  - Gmail;
  - Yahoo!;
  - Hotmail.
- Si vous possédez une adresse courriel gérée à partir d'un logiciel de courriel (par exemple, l'adresse courriel que vous offre votre fournisseur d'accès à Internet (FAI)), utilisez-en un muni d'un filtre performant.

<< Retour

5. Comment guérir?

Vous croyez avoir subi les contrecoups d'un pourriel malveillant? Voici ce que vous pouvez faire:

1. Installez tout de suite un pare-feu, pour éviter que ne problème ne prenne de l'ampleur.
2. Analysez votre ordinateur avec un logiciel antivirus.
   Supprimez les menaces détectées, s'il y en a.
3. Analysez votre ordinateur avec un logiciel antiespiogiciel .
   Supprimez les menaces détectées, s'il y en a.
4. Analysez votre ordinateur avec un deuxième logiciel antiespiogiciel.
   Supprimez les menaces détectées, s'il y en a.
5. Passez un petit coup de balai avec un logiciel « de ménage ».
   Supprimez les résidus détectés.

<< Retour

6. Sources documentaires

- 01net
- Assiste.com
- Branchez-vous!
- Grand dictionnaire terminologique
- Vunet.fr
- Wikipédia (français)
- Wikipedia (anglais)
- GRALLA, Preston. *PC Pest Control*, Sebastopol, O'Reilly Media Inc., 2005, 275 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet
Maîtrise en études françaises, cheminement communication et langages
Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Témoin traceur (*Tracking Cookie*)

Qu'est-ce que c'est?

« Je croyais pourtant que le *cookie* n'était pas dangereux. » serez-vous tenté de dire en consultant cette rubrique. Et vous avez raison. Le témoin, en tant que tel, est un petit fichier texte inoffensif implanté dans un ordinateur et permettant à un site Web, entre autres, de reconnaître un internaute lors d'une visite.

Tout se complique lorsque le témoin devient traceur; il collecte alors des renseignements (notamment sur les habitudes de navigation et sans le consentement de l'internaute observé), il les partage avec des sites partenaires (toujours à l'insu de l'internaute) et toutes les données recueillies servent souvent à envoyer de la publicité personnalisée.

Plus >>

Comment prévenir et comment guérir?

Comme l'objectif des témoins traceurs est de rester longtemps sur un ordinateur pour recueillir le plus de renseignements possible, ils ne se suppriment pas toujours de la même manière que les témoins traditionnels (qui peuvent être effacés avec l'aide du navigateur). Pour pallier à cette situation, la plupart des logiciels antiespiogiciels perçoivent les témoins traceurs comme des menaces potentielles et sont en mesure de les détecter et de les supprimer.

La procédure demeure la même : installez au moins deux logiciels antiespiogiciels, mettez religieusement à jour les signatures d'infection et scannez l'ordinateur une fois par semaine. De plus, pensez à télécharger un logiciel « de ménage » pour nettoyer plusieurs saletés et inutilités recueillies inconsciemment sur Internet.

En fin de compte, on pourrait comparer les témoins traceurs à de la poussière... Malgré tout notre bon travail de vigilance et d'entretien, elle finit toujours par réapparaître. Par conséquent, faites le ménage le plus souvent possible, plusieurs fois par semaine si nécessaire.

Plus >>

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Témoin traceur (*Tracking Cookie*)

1. Qu'est-ce que c'est?

Tel que mentionné à la page précédente, il ne faut pas confondre le témoin standard et le témoin traceur. Le témoin est un petit fichier texte inoffensif dont l'objectif est de recueillir certains renseignements pour permettre à un site Web de reconnaître un internaute et de lui offrir un service personnalisé. Le témoin traceur, quant à lui, va plus loin.

- Il recueille des renseignements, mais il peut en recueillir davantage que le témoin standard (notamment ceux sur les habitudes de navigation, un peu à l'image de l'espiogiciel).
- Les renseignements recueillis servent à un site Web précis, mais ils sont également remis à d'autres sites Web partenaires, partenariat habituellement inconnu des visiteurs.

<< Retour

2. Comment ça fonctionne?

Comme il a été mentionné ci-haut, le témoin traceur a pour objectif de recueillir et de partager divers renseignements.

1. Discret et léger, il est installé sur un ordinateur lors d'une visite sur un site Web et il surveille les activités effectuées sur ce site;
2. Il recueille des renseignements. Plus il reste longtemps sur un ordinateur, plus il peut étaler sa collecte sur une longue période;
3. Ces renseignements peuvent être utilisés par le site qui les recueille, mais ils sont surtout partagés avec des sites partenaires, à l'insu des visiteurs.

Ce dernier point peut soulever d'importantes questions éthiques. Si un site Web se vante de ne recueillir aucun renseignement à des fins publicitaires, mais qu'en revanche il tire un quelconque bénéfice de renseignements recueillis avec un témoin traceur sur un autre site, il commet un acte fautif.

À quoi servent tous ces renseignements? D'abord, à dresser le profil d'un internaute selon les habitudes de navigation, les activités en ligne, etc. Par la suite, ce profil sera utilisé par une entreprise, ou un site partenaire, pour envoyer de la publicité personnalisée; c'est ce qu'on appelle le ciblage comportemental. D'ailleurs, certaines « entreprises » se spécialisent dans la création de tels profils d'internautes afin de les vendre, ce qui est très rentable.

IMPORTANT

Certaines opérations de ciblage comportemental sont conformes et d'autres ne le sont pas. Si un site énonce ses intentions de partage d'information dans ses conditions d'utilisation, il agit dans la conformité. Même s'il s'agit d'un acte à l'éthique parfois douteuse, ce n'est pas nécessairement un acte illégal.

<< Retour

3. Quelles en sont les conséquences?

Tant que les témoins traceurs s'en tiennent au domaine publicitaire, ils ne sont que des nuisances. En effet, l'acharnement publicitaire, même s'il est personnalisé, peut être irritant. Cependant, d'un point de vue éthique, ils sont douteux, surtout parce qu'ils permettent un partage d'information plus important que celui auquel l'internaute a consenti.

De plus, du point de vue de la confidentialité, le doute quant aux témoins traceurs est accentué, car certains renseignements recueillis peuvent servir un dessein qui va au-delà de la publicité, jusqu'au vol d'identité (dans les cas extrêmes).

<< Retour

4. Comment prévenir?

Nous avons l'habitude de supprimer les témoins installés sur notre ordinateur avec la fonction prévue à cet effet dans notre navigateur. Toutefois, supprimer les témoins traceurs n'est pas aussi simple... quoique ce n'est pas bien complexe.

Comme il a été dit à la page précédente, on peut comparer les témoins traceurs à de la poussière; malgré tout notre bon travail de vigilance et d'entretien, elle réussit toujours à se faufiler jusqu'à nous. Que faut-il faire alors? Utilisez les logiciels ci-dessous à bon escient :

- Au moins deux logiciels antiespiogiciels dont les signatures d'infection sont à jour. La plupart sont en mesure de détecter et d'éradiquer les témoins traceurs;
    - Pensez à scanner votre ordinateur avec chaque antiespiogiciel le plus souvent pas

possible, une fois par deux ou trois jours si c'est nécessaire.

ATTENTION :

Scanner votre ordinateur plusieurs fois par semaine avec chaque antiespiogiciel peut être nécessaire si :

- Votre ordinateur est ouvert et connecté à Internet durant de longues heures; ou
- Vous faites beaucoup de téléchargement (en tous genres).

- Un logiciel « de ménage », pour nettoyer votre ordinateur des éléments qui auraient échappé au radar des logiciels antiespiogiciels;
  - Pensez à scanner votre ordinateur et votre base de registre au moins une fois par semaine.

<< Retour

5. Comment guérir?

Vous craignez d'avoir plusieurs témoins traceurs sur votre ordinateur? Voici ce que vous pouvez faire:

1. Analysez votre ordinateur avec un logiciel antiespiogiciel .
   Supprimez les menaces détectées, s'il y en a.
2. Analysez votre ordinateur avec un deuxième logiciel antiespiogiciel.
   Supprimez les menaces détectées, s'il y en a.
3. Passez un petit coup d'aspirateur avec un logiciel « de ménage ».
   Supprimez les résidus détectés.

<< Retour

6. Sources documentaires

- Assiste.com
- Grand dictionnaire terminologique
- Internet Security Zone.com
- Le Jargon français
- Wikipedia (anglais)
- CHARTON, ÉRIC. *Spywares et virus : Protégez-vous des logiciels escrocs*, coll. « Kit Campus », Paris, CampusPress, 2005, 245 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour : 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

AIDE AU DIAGNOSTIC

Les menaces Internet sont si nombreuses et si variées qu'on en perd parfois son latin. Si certaines sont facilement reconnaissables, d'autres sont d'une subtilité ou d'une complexité déconcertantes. Difficile alors de garder une approche proactive ou d'être en mesure de régler des problèmes.

Bien sûr, il y a des spécialistes (un professionnel, le beau-frère, etc.) qui peuvent vous venir en aide, mais avoir un minimum d'autonomie peut vous permettre de sauver du temps, de l'énergie et peut-être de l'argent.

Besoin d'un coup de main pour acquérir des connaissances et ainsi, être en mesure d'établir un bon diagnostic? Consultez la liste de **questions et de réponses** qui correspond à votre situation : un moment de panique, une inquiétude ou une recherche de renseignements.

Besoin d'un autre coup de main pour éviter de retomber dans le piège? Créez une **liste personnalisée de bonnes habitudes et attitudes** à adopter sur Internet, liste que vous pourrez imprimer et garder à portée de vue pour vous ramener sur le bon chemin... virtuel.

Veuillez prendre note que les sources documentaires utilisées dans cette section peuvent être consultée en cliquant ici.

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

C'est la panique!

Pour avoir accès à la liste complète de ces sources documentaires utilisées dans cette page. cliquez ici.

Identité

Je me suis fait voler mon identité, que dois-je faire?

NE PAS PANIQUER

- **Problème :** Vous découvrez qu'on vous a volé votre identité, car :
  - une banque vous contacte à propos d'une demande d'ouverture de compte que vous n'avez jamais faite;
  - une institution vous contacte au sujet d'une demande de carte de crédit que vous n'avez pas formulée;
  - des transactions inconnues s'affichent sur vos relevés de compte (crédit, débit, etc.);
  - etc.
- **Causes probables :**
  - La cause peut être d'origine informatique. Un cheval de Troie ou un espiogiciel malicieux pourrait avoir recueilli vos renseignements confidentiels, à votre insu. Ces renseignements peuvent permettre à un pirate de commettre une fraude.
  - La cause peut être une arnaque informatique. L'hameçonnage est une technique de fraude misant sur la manipulation des victimes afin de recueillir des renseignements confidentiels.
  - Il se peut que la cause n'implique rien d'informatique. Un individu pourrait usurper vos renseignements confidentiels en volant vos papiers ou votre portefeuille, ou encore en fouillant dans votre bac à recyclage à la recherche de relevés de compte.
- **Solutions :**
  - Si on a tenté d'ouvrir un compte, de faire un emprunt ou de commettre tout autre acte en votre nom, contactez les institutions et organisations concernées pour leur expliquer que vous avez été victime de vol d'identité.
  - Contactez l'une de ces agences canadiennes de renseignements de crédit pour leur signaler que vous êtes à risque de subir une fraude et pour obtenir de l'aide :
    - TransUnion Canada
    - Equifax Canada
  - Au Québec, un organisme à but non lucratif, l'Institut de sécurité de l'information du Québec (ISIQ), fournit de l'information sur la protection de l'identité sur Internet. Consultez leurs rubriques pour plus de détails :
    - Qu'est-ce que le vol d'identité?
    - Êtes-vous victime de vol d'identité?
    - Quoi faire si vous êtes victime de vol d'identité?

Courriel

Je me suis fait pirater mon adresse courriel, que dois-je faire?

NE PAS PANIQUER

- **Problème :** Vous vous apercevez qu'un individu est entré dans votre compte. Il pourrait alors :
  - voler vos courriels;
  - vous menacer de supprimer vos courriels, communiquer de la fausse information à vos contacts, etc., si vous ne lui remettez pas un certain montant d'argent;
  - utiliser votre adresse courriel pour envoyer du pourriel ou des courriels d'hameçonnage;

- etc.

- **Solutions :**
  - Communiquez d'abord avec l'administration de votre service de courriel et leur faire part de votre problème. *Donnez le plus de détails possible. Voici les contacts des principaux services de courriel gratuits :*
    - Hotmail
    - Gmail
    - Yahoo! (choisissez l'option « Je pense que mon compte a été compromis »); si ce lien ne fonctionne pas, contactez-les à cette adresse.

    Et voici les contacts des principaux fournisseurs d'accès à Internet (FAI) de l'ouest québécois :
    - Bell Internet (anciennement Sympatico); si ce lien ne fonctionne pas, contactez-les à cette adresse.
    - Vidéotron
- Communiquez également avec l'organisme Phone Busters, ils seront en mesure de vous aider :
  - *Phone Busters*

Logiciels de sécurité (antivirus, antiespiogiciel, etc.)

Mon logiciel antivirus se désactive automatiquement, est-ce normal?

NON

- **Problème :** Sans raison apparente, votre logiciel antivirus se désactive de lui-même.
- **Causes probables :**
  - Il se peut que votre ordinateur soit infecté par un espiogiciel particulièrement malicieux.
  - Si ce n'est pas un espiogiciel, il se peut que ce soit un cheval de Troie.
  - Si ce n'est ni un espiogiciel ni un cheval de Troie, il se peut que ce soit un ver informatique.
- **Notes :**
  - Dans une telle situation, il est possible que votre ordinateur fasse partie d'un *botnet*. Ce dernier exploite les bandes passantes de plusieurs ordinateurs afin d'obtenir une superpuissance qui lui est nécessaire pour ses actes de grande envergure (envois massifs de pourriels ou de courriels d'hameçonnage, attaque contre un site Web, etc.).
  - Si vous croyez faire partie d'un *botnet*, voici ce que vous pouvez faire :
    1. Installer un pare-feu, pour éviter que le problème ne prenne de l'ampleur.
    2. Tout mettre en oeuvre pour détecter et supprimer l'espiogiciel (Comment guérir), le cheval de Troie (Comment guérir) ou le ver informatique (Comment guérir) à l'origine du problème.

Mes logiciels de sécurité ne démarrent plus, que dois-je faire?

NE PAS PANIQUER

- **Problèmes :**
  - Le logiciel antivirus et les autres logiciels de sécurité semblent avoir été automatiquement désactivés à votre insu.

- Vous n'arrivez pas à les réactiver.
- Tous les autres logiciels (suite bureautique, système d'exploitation, jeux, etc.) fonctionnent normalement.

- **Cause probable :** Il se peut que votre ordinateur soit infecté par un cheval de Troie.
- **Notes :**
  - Puisque l'ouverture des logiciels de sécurité conventionnels est compromise, il est suggéré de commencer avec une analyse antivirus en ligne :
    - Internet Explorer : ESET Nod32 (le plus performant)
    - Mozilla Firefox : TrendMicro (le plus accessible)
  - Par la suite, passez directement au mode sans échec et essayez de démarrer une analyse antivirus et une analyse antiespiogicielle.
  - Si le problème persiste toujours, visitez un forum pour obtenir une aide adaptée.

Un logiciel antivirus (ou un antiespiogiciel) inconnu est apparu et je n'arrive pas à le désinstaller. Que faire?

S'ARMER DE PATIENCE

- **Problèmes:**
  - Du jour au lendemain, vous remarquez qu'un logiciel antivirus (ou antiespiogiciel) **inconnu** vous propose d'éradiquer tous les parasites qui infestent votre ordinateur;
  - Malgré toutes vos analyses et tentatives d'éradication, vous n'arrivez pas à vous en débarrasser.
- **Cause probable :** Il se peut que votre ordinateur soit infecté par un faux logiciel de sécurité.
- **Notes :**
  - Supprimer un faux logiciel de sécurité n'est pas chose simple, raison pour laquelle il est indiqué de s'armer de patience.
  - Une méthode en plusieurs étapes vous est proposée dans la fiche descriptive du faux logiciel de sécurité (Comment guérir).
  - Les faux logiciels de sécurité sont en constante mutation afin de rendre leur détection et leur éradication toujours plus ardue. Les forums sont une bonne ressource pour obtenir de l'aide, car ils sont en mesure d'offrir des solutions adaptées et à jour.

Un logiciel antivirus (ou un antiespiogiciel) inconnu m'affiche des résultats alarmants, dois-je m'y fier?

NON

- **Problèmes :**
  - Un logiciel antivirus (ou antiespiogiciel) **inconnu** affiche des résultats d'analyse alarmants. Par exemple : « ATTENTION! 256 virus ont été détectés sur votre ordinateur! »;
  - Vous faites une analyse avec un « vrai » logiciel antivirus et avec deux « vrais » logiciels antiespiogiciels, vous n'obtenez pas de résultats aussi alarmants et le « faux » logiciel continue d'afficher des alertes.
- **Cause probable :** Il se peut que votre ordinateur soit infecté par un faux logiciel de sécurité.
- **Notes :**
  - Supprimer un faux logiciel de sécurité n'est pas chose simple, il faut s'armer de patience.
  - Une méthode en plusieurs étapes vous est proposée dans la fiche descriptive du faux logiciel de sécurité

(Comment guérir).

- Les faux logiciels de sécurité sont en constante mutation afin de rendre leur détection et leur éradication toujours plus ardue. Les forums sont une bonne ressource pour obtenir de l'aide, car ils sont en mesure d'offrir des solutions adaptées et à jour.

Votre ordinateur

Mon ordinateur redémarre à intervalles réguliers, est-ce je peux « arranger » ça?

OUI

- **Problèmes :**
  - Chaque fois que l'ordinateur est démarré, il fonctionne normalement pendant quelques minutes (10, 15, 20, etc.), puis il redémarre **de lui-même**, sans aucune demande de votre part;
  - Ce cercle vicieux ne semble pas avoir de fin.
- ***Causes probables :***
  - Il se peut que votre ordinateur soit infecté par un ver informatique.
  - Si ce n'est pas un ver informatique, il se peut que ce soit un cheval de Troie.
- **Note :** Tentez d'abord les méthodes d'éradication contre les vers informatiques (Comment guérir) et si le problème persiste, tentez celles contre les chevaux de Troie (Comment guérir).

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet
Maîtrise en études françaises, cheminement communication et langages
Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

Je suis inquiet... ou exaspéré

Pour avoir accès à la liste complète de ces sources documentaires utilisées dans cette page, cliquez ici.

Web

Fenêtre pop-up... Y'en a marre!

AH!

- **Problèmes :**
  - Dès que votre ordinateur se connecte à Internet, ou encore dès que vous ouvrez votre navigateur, des fenêtres pop-up apparaissent sur votre écran.
  - Si vous ne les fermez pas, elles vous empêchent carrément de naviguer sur le Web ou d'utiliser normalement votre ordinateur.
- **Cause probable :** Il se peut que votre ordinateur soit infecté par plusieurs espiogiciels et (ou) logiciels publicitaires.
- **Note :** Les logiciels permettant de trouver et d'éradiquer les espiogiciels ciblent également les logiciels publicitaires.

Internet Explorer plante régulièrement, que dois-je faire pour que ça cesse?

UNE MISE À JOUR

- **Problèmes :**
  - Sans raison apparente, le navigateur Internet Explorer plante en cours d'utilisation.
  - Vous n'éprouvez pas cette difficulté avec Mozilla Firefox.
- **Solutions :**
  - Tout d'abord, mettre à jour le système d'exploitation Windows, ce qui inclura systématiquement une mise à jour du navigateur Internet Explorer.
  - Si le problème persiste, il se peut alors qu'une **menace** en soit la cause.
    - Il se peut qu'un ou plusieurs espiogiciels aient infecté votre ordinateur.
    - Si malgré l'éradication des espiogiciels le problème persiste, il se peut que ce soit un cheval de Troie.
    - Tentez d'abord les méthodes d'éradication contre les espiogiciels (Comment guérir), puis celles contre les chevaux de Troie (Comment guérir).

ActiveX, est-ce que c'est une menace?

NON

ActiveX est un composant logiciel développé par Microsoft. Sur le Web, il est accessible uniquement par Internet Explorer. Il permet d'offrir aux pages Web plus de dynamisme, d'interactivité et de possibilités. Pour fonctionner, un composant ActiveX doit toutefois être téléchargé sur l'ordinateur de l'internaute.

Malheureusement, certains composants ActiveX démarrent également le téléchargement de logiciels malveillants. Pour cette raison, leur téléchargement peut être bloqué par le navigateur.

Si vous êtes sur un site de confiance, vous pouvez accepter le téléchargement du composant ActiveX, mais assurez-vous que votre pare-feu soit bien activé, au cas où un parasite tenterait tout de même de s'infiltrer. Si vous n'êtes pas sur un site de confiance, refusez. Vous ne pourrez pas voir certains contenus, mais vous serez un peu plus en sécurité.

Est-ce que je laisse des « traces » lorsque je navigue sur le Web?

OUI

Internet crée une illusion d'anonymat. Plusieurs internautes croient à tort qu'ils sont « invisibles » sur le réseau : aucune présence physique aux alentours, un écran en guise de barrière, la possibilité de se créer un personnage, etc.

Mais détrompez-vous. Vous laissez des traces lorsque vous naviguez. Adresse IP, témoins et autres historiques de votre navigation peuvent être récupérés par des tierces personnes.

Vous n'êtes pas anonymes sur Internet, puisqu'on peut vous repérer et pas seulement virtuellement; les traces laissées permettent de vous localiser physiquement.

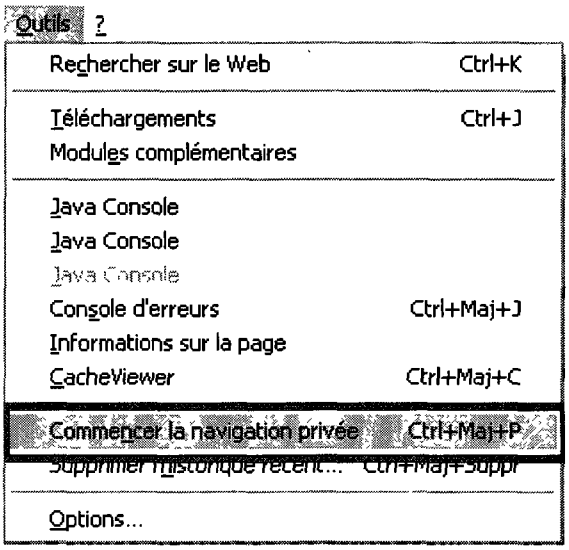
- Faites un test et découvrez les traces que vous laissez sur le Web!
    - Anonymat.org
- Vous souhaitez naviguer dans l'anonymat?
    - *The Cloak* (anglais).

Est-ce dangereux de faire des achats sur le Web?

SI ON FAIT PREUVE DE JUGEMENT, NON

Lorsqu'on fait des achats en ligne, il faut allier **prudence**, **jugement** et **carte de crédit**.

- **Prudence et jugement :** N'oubliez pas qu'en effectuant une transaction en ligne, vous envoyez dans des données bancaires personnelles le cyberespace. Vous devez donc tout mettre en œuvre pour qu'aucun individu n'intercepte vos données lors de leur voyage entre le point A (votre ordinateur) et le point B (le commerçant).
    - **De votre côté**, assurez-vous que votre pare-feu soit activé et bien paramétré au moment de la transaction;
    - **Toujours de votre côté**, utilisez la fonctionnalité « Navigation privée » offerte par plusieurs navigateurs (dont Internet Explorer et Mozilla Firefox). Une fois ce mode activé, le navigateur ne sauvegardera pas l'historique de votre navigation, ne conservera aucun témoin ni fichier temporaire et n'enregistrera pas les recherches. Pour démarrer la navigation privée dans Mozilla Firefox, cliquez sur le menu « Outils », puis sur le sous-menu « Commencer la navigation privée »;



- **Côté commerce**, assurez-vous que le site sur lequel vous magasinez offre une solution de paiement sécurisée, c'est-à-dire qui chiffre (ou crypte) vos données personnelles lors de la transaction. Par exemple, PayPal offre un tel service de chiffrement (pour en savoir plus, cliquez ici).

CULTURE GÉNÉRALE

Certains sites de commerce développent eux-mêmes d'excellentes solutions de paiement sécurisé (par exemple, Amazon). D'autres choisissent plutôt d'employer les services de sites spécialisés dans les transactions sécuritaires en ligne (par exemple, le site d'enchères eBay offre à ses membres de payer leurs achats avec PayPal).

ATTENTION

Ne faites pas vos achats sur des sites obscurs qui n'exhibent **aucune** solution de paiement sécurisé.

Dans la rue, vous refuseriez de donner votre numéro de carte de crédit à un individu à l'air louche, n'est-ce pas? C'est la même chose sur le Web. Pour mériter votre achat et votre paiement, un commerce en ligne doit vous **prouver** qu'il offre un service de paiement sécuritaire.

- **Carte de crédit :** Une fois votre transaction terminée, vous ne voulez pas qu'un individu ait accès à votre numéro de carte de crédit. Alors, effacez toutes les traces qui pourraient avoir conservé des indices, en totalité ou en partie, sur votre précieux numéro.
  1. Lorsque la transaction est terminée, fermez la session en utilisant le bouton à cet effet sur le site Web.
  2. Fermez la session de navigation privée.
  3. Si vous n'aviez pas démarré l'option « Navigation privée » ou si votre navigateur n'offre pas cette fonctionnalité, effacez vos traces en supprimant le contenu de votre mémoire cache, votre historique de votre navigation et vos témoins.
  4. Passez un petit coup de balai en utilisant un logiciel « de ménage ».
- **Note :** La prudence et le jugement sont tout aussi impératifs lors de l'utilisation d'un compte bancaire pour effectuer

des paiements en ligne.

Messagerie instantanée

Je reçois des messages étranges dans MSN Messenger/Windows Live Messenger, de quoi s'agit-il?

DE LA PUBLICITÉ

- **Problèmes :**
  - De temps à autre, une fenêtre de discussion apparaît, comme si un(e) ami(e) voulait clavarder avec vous, mais le message affiché n'a rien à voir avec l'ami(e) en question.
    Exemple de message : *Eh, click here to see who blocked you!* ou Salut! Va voir mes dernières photos en cliquant ici.
  - Le message contient habituellement un hyperlien.
  - L'ami(e) concerné(e) vous assure qu'il/elle ne vous a jamais envoyé ce message.
- **Cause probable :** Il se peut que votre ami(e) soit aux prises avec un ou plusieurs logiciels publicitaires. Si vous ne cliquez pas sur l'hyperlien contenu dans le message, vous ne « l'attraperez » pas.
- **Solutions :**
  - Écrivez un courriel à votre ami(e) pour lui signaler le problème. Il/elle ne sait probablement pas que ces messages sont envoyés en son nom.
  - Renseignez-vous sur les logiciels publicitaires (Qu'est-ce que c'est) et les trucs pour s'en débarrasser (Comment guérir). Parlez-en à votre ami(e)! ;-)
- **Note :** Profitez-en pour analyser votre propre situation (Comment prévenir et Comment guérir), peut-être avez-vous ce même problème et que vous l'ignorez...

Courriel

Les courriels véhiculent toutes sortes de renseignements. Comment savoir si ce qu'on nous raconte est vrai?

À VOUS DE LE DÉCOUVRIR

- **Problème :** Vous avez reçu un courriel qui :
  - Vous transmet de l'information un peu alarmiste.
    - Exemple : Hotmail est surchargé et deviendra payant sous peu!
  - Vous demande de transférer le courriel à un certain nombre de personnes pour éviter des conséquences fâcheuses :
    - Exemple : Envoyez ce courriel à 15 personnes et vous n'aurez pas à payer pour votre compte Hotmail!
- **Cause probable :** Vous avez probablement reçu un canular .
- **Solution :** À vous de distinguer les vrais courriels des faux. Renseignez-vous sur les moyens à prendre pour prévenir

les effets indésirables des canulars (Comment prévenir).

Logiciels de sécurité (antivirus, antiespiogiciel, etc.)

On m'affiche constamment de la publicité pour m'inciter à télécharger un logiciel de sécurité, est-ce fiable?

NON

- **Problèmes :**
  - Des boîtes publicitaires apparaissent fréquemment sur votre écran pour vous inciter à télécharger un logiciel de sécurité (par exemple, un logiciel antiespiogiciel).
  - Malgré toutes vos analyses antivirus et antespiogicielles, rien n'y fait, cette publicité est toujours présente.
- **Causes probables :**
  - Il se peut que votre ordinateur soit infecté par un ou plusieurs espiogiciels.
  - Si ce n'est pas un ou plusieurs espiogiciels, il se peut que ce soit un faux logiciel de sécurité.
- **Notes :**
  - N'oubliez pas que les concepteurs de logiciels de sécurité **crédibles** n'envahiront pas votre ordinateur pour vous proposer leurs produits, car cette méthode porterait atteinte à leur crédibilité. L'industrie des faux logiciels de sécurité et autres tromperies, quant à elle, n'hésitera pas à le faire.
  - Tentez d'abord les méthodes d'éradication contre les espiogiciels (Comment guérir) puis celles contre les faux logiciels de sécurité (Comment guérir).

Votre ordinateur et votre connexion Internet

Mon ordinateur prend du temps à démarrer, je n'en peux plus!

AH!

- **Problème :** Dès que vous appuyez sur le bouton « *Power* », l'ordinateur prend de 8 à 10 minutes, ou plus, pour démarrer complètement, c'est-à-dire jusqu'à ce que vous puissiez ouvrir un logiciel.
- **Causes probables :** Il se peut que votre ordinateur soit infecté par plusieurs espiogiciels et (ou) logiciels publicitaires.
- **Notes :**
  - Les logiciels permettant de trouver et d'éradiquer les espiogiciels ciblent également les logiciels publicitaires.
  - Si le démarrage de votre ordinateur au travail est lent, c'est en partie dû aux nombreux logiciels que les entreprises installent sur les ordinateurs des employés. Ils doivent tous s'activer au démarrage, ce qui ralentit le processus. Toutefois, la présence d'espiogiciels et (ou) de logiciels publicitaires peut contribuer à le ralentir davantage.

Les lumières du modem qui clignotent sans cesse, même si je ne fais rien sur mon ordinateur, est-ce normal?

NON

- **Symptômes :**
  - Vous fermez tous les logiciels actifs sur votre ordinateur; il n'y a que le système d'exploitation qui roule, et peut-être votre logiciel antivirus. Malgré tout, les lumières de votre modem clignotent comme un sapin de Noël le soir du 24 décembre.
  - Lorsque vous utilisez Internet, vous ne remarquez rien de grave, si ce n'est que quelques ralentissements.
  - Si votre ordinateur est connecté à un réseau, vous remarquez ces mêmes problèmes alors que votre machine est la seule à être active.
- **Causes probables :**
  - Il se peut que votre ordinateur soit infecté par un espiogiciel.
  - Si ce n'est pas un espiogiciel, il se peut que ce soit un ver informatique.
  - Si ce n'est ni un espiogiciel ni un ver informatique, il se peut que ce soit un cheval de Troie.

    Dans un cas comme dans l'autre, le logiciel malveillant risque d'avoir transformé votre ordinateur en zombie.

    Si tel est le cas, il est possible que votre ordinateur fasse partie d'un *botnet*. Ce dernier exploite les bandes passantes de plusieurs ordinateurs afin d'obtenir une superpuissance qui lui est nécessaire pour ses actes de grande envergure (envois massifs de pourriels ou de courriels d'hameçonnage, attaque contre un site Web, etc.).
- **Notes :**
  - Si vous croyez que votre ordinateur fait partie d'un *botnet*, voici ce que vous pouvez faire :
    1. Installer un pare-feu, pour éviter que le problème ne prenne de l'ampleur.
    2. Tout mettre en oeuvre pour détecter et supprimer l'espiogiciel (Comment guérir), le ver informatique (Comment guérir) ou le cheval de Troie (Comment guérir) à l'origine du problème.
  - Fait à noter, lorsque vous utilisez Internet, il est normal que les lumières de votre modem clignotent. Cela signifie que des données circulent entre votre ordinateur (ou réseau à domicile) et Internet. Si vous n'utilisez pas Internet, il se peut qu'elles clignotent un peu. Dans une situation d'inactivité, ce n'est pas normal si elles clignotent à un rythme effréné.

J'ai trouvé une clé USB abandonnée. Est-ce que l'utiliser est risqué?

OUI, POTENTIELLEMENT

La clé USB trouvée pourrait en effet contenir un logiciel malveillant qui se ferait un plaisir de visiter votre ordinateur au moment du branchement. Vous croyez que ça n'arrive qu'aux autres? Détrompez-vous... Ceux qui sont à l'origine de ces clés USB infectées misent sur la **curiosité** des individus pour propager leurs logiciels malveillants.

Que faut-il donc faire?

1. **Vous avez un deuxième ordinateur que vous utilisez peu?**

   La solution idéale serait de brancher la clé à un « ordinateur test », c'est-à-dire une machine secondaire que vous

utilisez peu, munie de tous les logiciels de sécurité nécessaires : logiciels antivirus et antiespiogiciels à jour, ainsi qu'un pare-feu. Branchez la clé USB, scannez-la avec les logiciels antivirus et antiespiogiciels et si tout est beau, vous pourrez l'utiliser.

De cette manière, s'il y a effectivement un logiciel malveillant sur l'appareil, vous le saurez et les dommages n'affecteront que votre machine secondaire. Si elle est branchée à un réseau, il est préférable de la déconnecter avant la procédure.

2. **Vous n'avez pas de deuxième ordinateur?**

Évitez de prendre des risques inutiles. L'humain est de nature curieuse et le désir d'utiliser la clé USB trouvée est compréhensible, mais gardez en mémoire que cet acte est **risqué**. Les clés USB sont très abordables de nos jours. Débarrassez-vous de celle que vous avez trouvée et achetez une clé neuve, c'est plus sécuritaire.

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet
Maîtrise en études françaises, cheminement communication et langages
Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Je veux me renseigner

Pour avoir accès à la liste complète de ces sources documentaires utilisées dans cette page, cliquez ici.

Web

Internet Explorer ou Mozilla Firefox?

VOUS FAITES BIEN DE POSER LA QUESTION

Internet Explorer et Mozilla Firefox sont deux navigateurs . Le premier est le plus utilisé, donc le plus populaire, et le second s'impose de plus en plus parmi le 1,8 milliard d'internautes*.

On pourrait avancer qu'Internet Explorer est victime de sa popularité. En effet, il existe plusieurs menaces qui cherchent à atteindre le plus d'ordinateurs possible pour des attaques de grande envergure. Le navigateur le plus populaire, utilisé par près de 61 %** de la population internaute, devient alors une « porte d'entrée » très profitable pour les pirates.

En utilisant des logiciels moins populaires, un internaute diminue le risque d'être atteint par ces attaques de masse. Mais attention, il n'élimine pas le risque, il le diminue.

Pour cette raison, l'utilisation de Mozilla Firefox pour la navigation Web en général devient intéressante. Il ne s'agit pas d'une protection miracle, mais elle permet de réduire le risque. De plus, ce navigateur est gratuit, stable, performant et facile à utiliser Ne désinstallez cependant pas Internet Explorer, vous pourriez en avoir besoin. En effet, certains sites (et certaines applications Web) ne fonctionnent que sur Internet Explorer.

- Téléchargez le navigateur Mozilla Firefox

Soit dit en passant, Mozilla Firefox n'est pas le seul navigateur alternatif disponible. Google Chrome et Opera sont deux autres excellents navigateurs gratuits, performants et simples d'utilisation.

- Téléchargez le navigateur Google Chrome
- Téléchargez le navigateur Opera

Laissez-vous également tenter par quelques logiciels de rechange aux logiciels plus populaires, il en existe plusieurs qui n'attendent qu'à être téléchargés :

- Logiciels de rechange.

* Internet World Stats
** MarketShare, division de Net Applications, avril 2009

Je n'ai absolument rien sur mon ordinateur qui pourrait intéresser un pirate. Pourquoi devrais-je me protéger autant?

C'est faux. Chaque internaute possède quelque chose qui intéresse les pirates.

Vous ne possédez peut-être pas de documents top-secrets de la NASA ou la recette pour guérir le cancer, mais vous avez... vos renseignements confidentiels. Nom, prénom, numéro de téléphone, adresse courriel, nom d'utilisateur, mot de passe, numéros de compte bancaire, de carte de crédit ou d'assurance sociale, voilà ce que les pirates cherchent. Et bien souvent, ils réussiront à les recueillir à votre insu.

Par exemple, ils pourraient installer sur votre ordinateur un espiogiciel de type enregistreur de frappe. Alors, si vous visitez le site de votre banque, il pourrait enregistrer votre numéro de compte et votre mot de passe au moment où vous les inscrirez, pour ensuite permettre à un ou plusieurs pirates de les utiliser. Un cheval de Troie pourrait permettre à un pirate d'infiltrer votre ordinateur à la recherche de précieux renseignements.

Pourquoi veulent-ils mettre la main sur ce type de renseignements? Parce qu'ils sont payants. Ils peuvent en effet être utilisés à différentes sauces : ciblage comportemental, vol d'argent, vol d'identité et autres magouilles potentiellement rentables.

Même si j'assure ma protection sur Internet, il se peut qu'un site Web légal avec qui je fais affaire cause ma perte. À quoi bon me protéger?

Lorsqu'on est confronté à des nouvelles comme celles ci-dessous, il est compréhensible que l'on se pose des questions :

- Une banque a « perdu » les données financières de milliers de clients utilisant son site Web;
- Un populaire moteur de recherche a été piraté;
- Un grand portail, pourtant reconnu comme étant un site de confiance, a été piraté, ce qui a entraîné l'infiltration de logiciels malveillants sur les ordinateurs de ses visiteurs.

Il ne faut pas oublier que l'ordinateur le plus sécuritaire au monde est un ordinateur éteint. Dès qu'il est démarré et connecté à Internet, il devient une source de risques.

Internet est un *Far West* rempli de bons et de vilains personnages. Certains volent des banques ou cherchent à arnaquer, d'autres sont agréables et offrent aide et information. Dans ce contexte, tout ce qui est actif sur Internet, qu'il s'agisse d'un internaute ou d'un site Web, est potentiellement à risque de subir les assauts des vilains.

En tant qu'internaute, vous avez le choix. Vous pouvez fermer les yeux et croire que peu importe ce qui arrive, vous aurez des problèmes. Ou encore, vous pouvez ouvrir les yeux et éviter le plus de problèmes possible en vous sensibilisant. Après tout, mieux vaut être **proactif** et éviter les problèmes que **réactif** et être pris au dépourvu.

CULTURE GÉNÉRALE

On peut comparer la situation d'un internaute sur le réseau à celle d'un automobiliste sur l'autoroute. Il peut y conduire les yeux fermés et peut-être qu'avec une sacrée chance, il évitera un accident. Ou encore, il peut garder les yeux ouverts, faire attention et se munir d'une bonne police d'assurance; le risque d'accident s'en trouve réduit et s'il survient, il sera préparé.

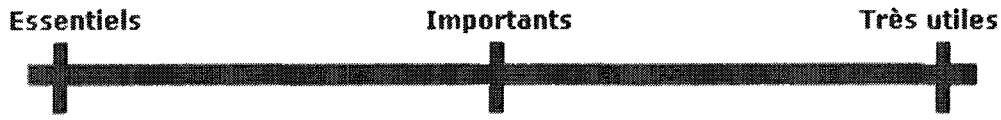
Logiciels de sécurité (antivirus, antiespiogiciel, etc.)

De quels logiciels ai-je besoin pour assurer ma sécurité?

QUELLE BONNE QUESTION

Il existe une série de logiciels qu'on peut qualifier d'« essentiels » à la sécurité d'un ordinateur personnel. Certains internautes seraient tentés de ne pas les installer, pour de multiples raisons, mais c'est imprudent, car le risque s'en trouve alors grandement augmenté.

Une fois la base logicielle assurée, d'autres logiciels « importants » et « très utiles » contribuent à renforcer la sécurité d'un ordinateur personnel, tout ça pour diminuer le risque. Ils ne l'éliminent pas, mais il contribuent à le tenir à distance.



- Un pare-feu
- Un logiciel antivirus
- Au moins deux logiciels antiespiogiciels

- Un logiciel « de ménage »
- Un logiciel *antirootkit*
- Une protection antiespiogicielle en temps réel
- Quelques logiciels de rechange :
  - Un navigateur autre qu'Internet Explorer
  - Un logiciel de courriel autre qu'Outlook
  - Un logiciel de messagerie instantanée autre que MSN Messenger/Windows Live Messenger
  - Un logiciel de lecture des PDF autre qu'Adobe Reader

- Un logiciel de désinstallation;
- D'autres logiciels de rechange

Quel logiciel antivirus devrais-je me procurer?

QUELLE BONNE QUESTION

Un logiciel antivirus efficace à 100 % pour tous les internautes, ça n'existe pas. Chaque ordinateur est unique, chaque usager en a une utilisation bien personnelle et les besoins et critères de chacun sont tout aussi personnels. Vous devez alors mener votre propre enquête pour déterminer quel logiciel antivirus **vous** conviendra.

Posez-vous les questions suivantes :

1. **Est-ce que je cherche un logiciel antivirus gratuit ou payant?**

   Contrairement à une croyance populaire, les logiciels gratuits sont très efficaces. Toutefois, les logiciels payants ont l'avantage d'offrir une interface souvent plus conviviale, des services supplémentaires, ou encore un plus grand nombre de produits connexes.

2. **Mise à part la protection antivirus, de quelle(s) protection(s) ai-je besoin?**

La grande majorité des logiciels antivirus offrent désormais toutes sortes de protections complémentaires. Établissez la liste de protections complémentaires dont vous avez besoin. Votre magasinage en sera facilité, puisque vous pourrez plus facilement « filtrer » la panoplie de produits offerts.

Exemples de protections complémentaires : logiciels antiespiogiciels (*anti-spyware*), pare-feu (*firewall*), filtre de pourriel (*spam filter*), protection antihameçonnage (*anti-phishing*), etc.

3. **Est-ce que j'ai des critères particuliers?**

   Établissez une liste de critères, cela vous permettra de faciliter davantage votre « magasinage ». Vous serez alors en mesure de poser les bonnes questions à un vendeur ou de repérer plus facilement ce qui vous intéresse sur le Web.

   Exemples de critères :

   - Un logiciel léger qui ne ralentira pas le fonctionnement de mon ordinateur;
   - Un logiciel offrant la mise à jour automatique des signatures d'infection;
   - Un logiciel offrant une barre d'outils accessible à partir de mon navigateur;
   - Etc.

Note : N'hésitez pas à consulter les rapports annuels du site AV-Comparatives.org, qui teste annuellement les logiciels antivirus (majoritairement payants) disponibles sur le marché.

- Rapports annuels d'AV-Comparatives.org (anglais)

Plusieurs logiciels antivirus sur un ordinateur, oui ou non?

NON

- **Pourquoi?** Dès qu'il y a plus d'un logiciel antivirus sur un ordinateur, ils peuvent entrer en conflit.

  Prenons l'exemple d'un ordinateur avec deux logiciels antivirus, « AV1 » et « AV2 ».

  - « AV1 » pourrait détecter « AV2 » comme une potentielle menace; ou encore
  - « AV1 » pourrait détecter un fichier nécessaire au fonctionnement d'« AV2 » et le supprimer. S'ils se « font le coup » mutuellement, les deux logiciels ne fonctionneront pas et l'ordinateur se trouvera sans aucune protection antivirus.

- **Note :** Si vous avez déjà un logiciel antivirus et que vous tentez d'en installer un 2^{e}, il se peut que cela ne fonctionne pas. Le premier antivirus pourrait effectivement bloquer cette installation. Toutefois, même si vous réussissez, désinstallez-en un. Il est important de n'avoir qu'un seul logiciel antivirus par ordinateur.

Plusieurs pare-feu sur un ordinateur, oui ou non?

NON

- **Pourquoi?** Dès qu'il y a plusieurs pare-feu sur un ordinateur, ils peuvent entrer en conflit.

  Tous les pare-feu filtrent les données entrantes, qui passent d'Internet à votre ordinateur, afin de bloquer, au maximum de leurs capacités, l'infiltration de parasites. La majorité d'entre eux filtrent également les données sortantes, qui passent de votre ordinateur à Internet.

Avoir deux pare-feu n'assure pas une « double » protection. Ce qui est bloqué par l'un pourrait passer au travers du filtre de l'autre et la protection de l'ordinateur en serait compromise.

- **Notes :**
  - Les routeurs et les concentrateurs (*hubs*) peuvent agir en tant que pare-feu **matériels**. Joindre un pare-feu matériel à un pare-feu logiciel est une bonne chose et il n'y aura pas de conflit, puisque l'un est à l'extérieur du boîtier de l'ordinateur et l'autre, à l'intérieur.
  - Avant d'installer un pare-feu, vérifiez si votre logiciel antivirus en offre déjà un.
  - Le système d'exploitation Windows comporte un pare-feu intégré. Pour en savoir plus sur sa désactivation ou sur sa gestion, si vous souhaitez l'utiliser, consultez la fiche Gestion du pare-feu Windows.

Plusieurs logiciels antiespiogiciels sur un ordinateur, oui ou non?

OUI

- **Pourquoi?** L'objectif du logiciel antiespiogiciel est d'éradiquer des parasites qui permettent de recueillir des données servant à envoyer de la publicité. C'est un domaine très rentable et plusieurs entreprises n'hésiteront pas à tenter de soudoyer les concepteurs d'antiespiogiciels (avec ou sans succès) pour que leurs mouchards échappent au radar.

  Avec deux logiciels antiespiogiciels, on augmente nos chances d'éradication; ce que l'un omettra de trouver pourra être découvert par un autre.

- **Note :** Gardez en mémoire que vous ne devez installer qu'un seul logiciel antivirus et un seul pare-feu; pour ce qui est des antiespiogiciels, un c'est bien, mais deux c'est mieux.

Lorsque mon logiciel antivirus (ou antiespiogiciel) détecte un logiciel malveillant, est-ce que ça signifie que mon *ordinateur est infecté?*

NON, IL NE L'EST PLUS

Pourquoi? Si votre logiciel antivirus (ou antiespiogiciel) détecte un logiciel malveillant, il se charge immédiatement de le neutraliser en le mettant en quarantaine ou en le supprimant.

Bref, dès qu'une menace est détectée, elle est prise en charge. Tant qu'elle n'est pas détectée, elle peut faire des dommages. Alors plus vous analysez fréquemment votre ordinateur, plus vous augmentez les chances de détection et plus il est en sécurité.

Votre ordinateur

J'ai entendu dire que dans Windows, un compte Utilisateur est plus sécuritaire qu'un compte Administrateur. Est-ce vrai?

OUI, MAIS IL FAUT FAIRE PLACE À LA NUANCE

Tout d'abord, une petite définition s'impose.

Lorsqu'on ouvre un ordinateur muni du système d'exploitation Windows, toutes versions confondues, on active un compte. Windows permet la création de plusieurs comptes, ce qui donne la possibilité à plusieurs personnes d'avoir un « espace » personnel sur la machine.

Il existe différents types de comptes :

- Il y a d'abord le « vrai » compte Administrateur, celui où vous n'allez presque jamais et qui vous permet de modifier et gérer tout ce qui existe sur l'ordinateur. Difficile d'accès, vous ne pouvez pas y accéder comme bon vous semble et c'est mieux ainsi, car le risque d'erreur y est grand si l'on ne connaît pas ses forces et ses faiblesses.
- Il y a ensuite l'autre compte Administrateur. À la base, c'est-à-dire lorsque Windows vient tout juste d'être installé, le premier usager d'un ordinateur en est également l'Administrateur.
    - **Avantage :** il offre plus de droits, donc il peut gérer plus aisément les logiciels, les périphériques et les mises à jour.
    - **Inconvénient :** il augmente le risque d'attaque. Certaines menaces, comme le *rootkit* et le cheval de Troie, ont besoin des droits administrateurs pour atteindre leurs objectifs.
- Il y a finalement le compte Utilisateur, qui limite l'utilisation dans ses actions possibles (entre autres, il ne permet pas l'installation de logiciels) et qui est donc plus sécuritaire.

Alors, est-ce mieux d'être sous un compte Administrateur ou Utilisateur? Il y a deux façons de voir ce « problème ».

1. **Vous avez un ordinateur blindé, c'est-à-dire :**
    - Un ordinateur muni d'un bon logiciel antivirus à jour, de logiciels antiespiogiciels à jour, d'une protection antiespiogicielle en temps réel et d'un pare-feu bien paramétré;
    - Vous mettez régulièrement à jour votre système d'exploitation, votre navigateur et votre logiciel de courriel;
    - Vous faites attention aux sites que vous visitez;
    - Vous évitez le téléchargement à partir d'un logiciel de pair-à-pair ou de toute autre source non fiable.

    Vous pouvez continuer d'utiliser un compte Administrateur, puisque vous êtes bien protégé. Bien évidemment, avoir un compte Utilisateur serait encore plus sécuritaire pour les activités telles que la navigation, l'utilisation d'un logiciel de courriel ou le travail avec une suite bureautique, mais la bonne protection (avec les logiciels mentionnés ci-haut) réduit le risque.

2. **Vous portez plus ou moins attention à la sécurité de votre ordinateur, ce qui est vrai si au moins l'une de ces situations s'applique à votre cas :**
    - Vous n'avez pas de logiciel antivirus ni de logiciels antiespiogiciels, ou si vous en avez, vous ne les avez pas mis à jour depuis un certain temps;
    - Vous n'avez pas de pare-feu;
    - Vous mettez rarement à jour votre système d'exploitation, votre navigateur ou votre logiciel de courriel;
    - Vous avez une navigation plus ou moins sécuritaire?
    - Vous utilisez un logiciel de pair-à-pair.

    Il est alors préférable de vous créer un compte Utilisateur. Vous voulez naviguer, utiliser votre logiciel de courriel, travailler, utiliser un logiciel de pair-à-pair, faire une utilisation normale d'un ordinateur? Utilisez votre compte Utilisateur. Vous devez installer un logiciel? Utilisez votre compte Administrateur. Soit dit en passant, vous aurez accès à tous les logiciels installés dans votre compte Utilisateur.

Besoin de détails supplémentaires sur la gestion des comptes de Windows?

- Le site de Malekal a toute l'information dont vous avez besoin.

Est-ce vraiment utile de faire des sauvegardes (*backups*)?

OUI

- **Pourquoi?** Personne n'est à l'abri d'un formatage du disque dur. Que ce soit en raison d'un vilain logiciel malveillant qui a fait des dommages irréparables, ou encore d'une mauvaise configuration qui a bousillé le système d'exploitation, un formatage peut être inévitable.

  Vos fichiers seront tous supprimés. Vous serez alors bien heureux de les avoir sauvegardés sur un lecteur externe (DVD, CD, disque dur externe, clé USB, disquette, etc.).

- **Note :**
  - Faites régulièrement des sauvegardes, une fois par semaine de préférence ou deux fois par mois. Ou encore, faites-en une juste avant une opération risquée (désinstaller un logiciel malveillant, etc.).
  - Il est suggéré de faire des sauvegardes de vos fichiers (documents, MP3, photos, etc.) sur un lecteur externe (DVD, CD, disque dur externe, clé USB, disquette, etc.). Comment y arrive-t-on?
    - Pour faire une sauvegarde sur un CD ou un DVD, ouvrez le logiciel que vous utilisez pour graver des CD/DVD (Nero, Sonic, etc.) et créez un CD ou un DVD **de données**.
    - Pour faire une sauvegarde sur un disque dur externe, une clé USB ou une disquette, branchez le lecteur à votre ordinateur (ou insérez la disquette dans le lecteur prévu à cet effet). Ouvrez ensuite le Poste de travail (ou Ordinateur sous Windows Vista et Windows 7) et double-cliquez sur l'icône représentant votre lecteur externe. Utilisez par la suite le bon vieux copier-coller pour transférer tous vos fichiers sur le lecteur externe.
    - Si votre lecteur externe offre un logiciel de gestion des transferts, utilisez-le pour vos sauvegardes.
  - Pour vos logiciels, gardez précieusement tous les CD ou DVD qui ont servi à leur installation. Il vous suffira de les réinstaller après le formatage.

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

Sécurité Internet 101 >> Liste de bonnes habitudes et attitudes - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

http://pages.usherbrooke.ca/securite_internet101/liste/checklist.html

Les plus visités BDI

Sécurité Internet 101 >> Liste de bo...

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Questions Réponses
C'est la panique
Je suis inquiet
Je veux me renseigner

Bonnes habitudes et attitudes à emporter!
Liste personnalisée
Instructions
Note

LISTE PERSONNALISEE DE BONNES HABITUDES ET ATTITUDES

Plénitude, béatitude, amplitude, gratitude... Tels sont quelques mots que nous pouvons utiliser pour décrire Internet et il y en a d'autres. Vis-à-vis de ces sollicitudes se trouvent les bonnes habitudes et attitudes sans lesquelles tout aptitude tombera rapidement en désuétude.

En effet, ces bonnes habitudes et attitudes sur Internet sont essentielles pour renforcer **votre protection et celle des gens avec qui vous communiquez** sur Internet. Car si vous êtes dangereux pour votre propre personne, vous pouvez également représenter un risque pour vos contacts.

Besoin d'un aide mémoire? Utilisez la liste ci-dessous. Quoi de plus pratique au chevet de votre ordinateur...

1. Inscrivez votre nom dans le champ prévu à cet effet. Ce renseignement ne sera pas recueilli. Il ne sert qu'à personnaliser votre liste.
2. Observez les catégories de bonnes habitudes et attitudes.
3. Cochez celles qui vous semblent importantes.
4. Dès que vous cochez une catégorie, plusieurs conseils apparaissent. Observez-les attentivement et cochez ceux que vous souhaitez ajouter à votre aide mémoire.
5. Lorsque vous avez fait vos choix, cliquez sur "Donnez-moi ma liste".
6. Et voilà! Il ne vous reste qu'à l'imprimer.

Inscrire votre prénom

☐ **Bonnes habitudes et attitudes avec mon ordinateur**

☐ **Bonnes habitudes et attitudes avec mes logiciels**

☐ ***Bonnes habitudes et attitudes avec mon courriel***

☐ **Bonnes habitudes et attitudes sur le site de ma banque**

☐ **Bonnes habitudes et attitudes si j'utilise un logiciel de pair-à-pair (*P2P*)**

☐ **Bonnes habitudes et attitudes sur les sites de réseautage social**

Terminé

Sécurité Internet 101 >> Liste de bonnes habitudes et attitudes - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

http://pages.usherbrooke.ca/securite_internet101/liste/checklist.html

Les plus visités BDI

Sécurité Internet 101 >> Liste de bo...

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Questions Réponses
C'est la panique
Je suis inquiet
Je veux me renseigner

Bonnes habitudes et attitudes à emporter!
Liste personnalisée
Instructions
Note importante

LISTE PERSONNALISEE DE BONNES HABITUDES ET ATTITUDES

Plénitude, béatitude, amplitude, gratitude... Tels sont quelques mots que nous pouvons utiliser pour décrire Internet et il y en a d'autres. Vis-à-vis de ces sollicitudes se trouvent les bonnes habitudes et attitudes sans lesquelles tout aptitude tombera rapidement en désuétude.

En effet, ces bonnes habitudes et attitudes sur Internet sont essentielles pour renforcer **votre protection et celle des gens avec qui vous communiquez** sur Internet. Car si vous êtes dangereux pour votre propre personne, vous pouvez également représenter un risque pour vos contacts.

Besoin d'un aide mémoire? Utilisez la liste ci-dessous. Quoi de plus pratique au chevet de votre ordinateur...

Ces suggestions de bonnes habitudes et attitudes concernent les problèmes technologiques liés à l'utilisation d'Internet et ce qui inclut la *protection des données confidentielles des internautes* et l'usage sur cet objet avec ... Les problèmes de nature sociale occasionnés en tout ou en partie par Internet (pédophilie, ... pornographie, etc.) ne font pas partie de ces listes.

Attention ... Cochez

Inscrire votre prénom

☐ **Bonnes habitudes et attitudes avec mon ordinateur**

☐ **Bonnes habitudes et attitudes avec mes logiciels**

☐ **Bonnes habitudes et attitudes avec mon courriel**

☐ **Bonnes habitudes et attitudes sur le site de ma banque**

☐ **Bonnes habitudes et attitudes si j'utilise un logiciel de pair-à-pair (*P2P*)**

☐ **Bonnes habitudes et attitudes sur les sites de réseautage social**

Terminé

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Liste personnalisée de bonnes habitudes et attitudes

Plénitude, béatitude, amplitude, gratitude... Tels sont quelques mots que nous pouvons utiliser pour décrire Internet, et il y en a d'autres. Vis-à-vis de ces sollicitudes, se trouvent les bonnes habitudes et attitudes, sans lesquelles tout aptitude tomberait rapidement en désuétude.

En effet, ces bonnes habitudes et attitudes sur Internet sont essentielles pour renforcer **votre** protection et **celle des gens avec qui vous communiquez** sur Internet. Car si vous êtes dangereux pour votre propre personne, vous pouvez également représenter un risque pour vos contacts.

Besoin d'un aide-mémoire? Utilisez la liste ci-dessous. Quoi de plus pratique au chevet de votre ordinateur!

Pour bien personnaliser votre liste, vous être invité à inscrire votre prénom :

Annie

Attention, prêts... Cochez!

☑ **Bonnes habitudes et attitudes... avec mon ordinateur**

- ☑ Ma vigilance est toujours de mise, car je suis responsable de ma sécurité et je suis impliqué dans celle de mon entourage __
  On peut comparer Internet à une autoroute. Vous êtes un automobiliste parmi tant d'autres sur cette autoroute. Si vous n'êtes pas suffisamment vigilant, vous pouvez avoir un accident et vous ne serez pas la seule personne à en subir les conséquences.
- ☑ Je prends le temps d'apprendre comment fonctionne mon ordinateur
- ☑ Je m'assure que mon systeme d'exploitation est à jour __
  Windows offre une fonction de mise à jour automatique (qui est habituellement activée par défaut). Windows se charge alors de la recherche et de l'installation des les mises à jour nécessaires.

  Ce processus est énergivore et il peut ralentir le fonctionnement de votre ordinateur, mais c'est un « mal nécessaire ». Ces mises à jour sont essentielles pour colmater les failles du système d'exploitation qui pourraient permettre l'infiltration de logiciels malveillants.
- ☑ Je fais régulièrement des sauvegardes (*backups*) de mes fichiers importants __
  Si vous devez formater votre disque dur, vous aurez alors accès aux copies sauvegardées.
- ☑ Si j'éprouve une difficulté, je ne panique pas et je fais preuve de patience __
  Si vous êtes calme, vous serez en meilleure position pour trouver une solution ou une piste de solution.

☑ **Bonnes habitudes et attitudes... avec mes logiciels**

☑ Dès que je me connecte, je m'assure que mon pare-feu est activé et bien paramétré. __
Contrairement à ce qu'on pourrait croire, paramétrer un pare-feu n'a rien de sorcier. Lors de votre utilisation d'Internet, il fera apparaître des boîtes de dialogue qui se chargeront de ce paramétrage en vous demandant si vous autorisez (ou refusez) le transfert de données effectué par un logiciel ou un service. Votre décision sera alors enregistrée sous forme de règle et votre pare-feu la respectera à l'avenir.

Si des questions surgissent en cours d'utilisation, consultez l'aide du logiciel, une fonctionnalité méconnue (ou mal-aimée), mais pourtant très utile.

☑ Dès que je me connecte, je m'assure que mon logiciel antivirus est bien activé.

☑ Je pense à scanner mon ordinateur avec mon logiciel antivirus au moins deux fois par mois.

☑ Je fais une mise à jour des signatures d'infection de mon logiciel antivirus le plus souvent possible, une fois par semaine si nécessaire. __
Plusieurs logiciels antivirus offrent un service de mise à jour automatique des signatures d'infection. Vérifiez si le vôtre contient une telle fonctionnalité, bien utile en cas d'oubli.

Si les signatures d'infection d'un logiciel antivirus ne sont pas à jour, l'efficacité du logiciel est remise en question, puisqu'il n'est plus en mesure de detecter les plus récentes menaces.

☑ J'ai installé au moins deux logiciels antiespiogiciels sur mon ordinateur.

☑ Je pense à scanner mon ordinateur avec chaque logiciel antiespiogiciel au moins une fois par semaine.

☑ Je fais une mise à jour des signatures d'infection de mes logiciels antiespiogiciels le plus souvent possible, une fois par semaine si nécessaire. __
Si les signatures d'infection d'un logiciel antiespiogiciel ne sont pas à jour, l'efficacité du logiciel est remise en question, puisqu'il n'est plus en mesure de détecter les plus récentes menaces.

☑ J'ai une protection antiespiogicielle en temps réel et je m'assure qu'elle est activée en tout temps.

☑ J'ai installé un logiciel « de ménage » et je l'utilise régulièrement, une fois par semaine si nécessaire.

☑ Je mets mon navigateur à jour lorsque nécessaire (par exemple, à l'affichage d'un avis de mise à jour). __
Il se peut que les mises à jour de votre navigateur s'installent automatiquement (par exemple, les mises à jour d'Internet Explorer s'installent en même temps que celles de Windows, par le service Windows Update). Si tel est le cas, n'arrêtez pas le processus d'installation lorsqu'il s'active.

Le navigateur, peu importe son concepteur, est un logiciel qui contient des failles. Un logiciel malveillant peut alors exploiter l'une de ces failles pour s'infiltrer dans un ordinateur.

Les mises à jour comprennent habituellement des correctifs de sécurité visant à colmater les failles au fur et à mesure qu'elles sont découvertes, ce qui réduit les risques d'infiltration.

☑ J'ai créé un cédérom de sécurité contenant les fichiers d'installation de tous les logiciels de sécurité installés. __
Pourquoi créer un tel cédérom? Si vos logiciels de sécurité ne répondent plus à la suite d'une attaque ou d'un mauvais paramétrage, vous serez alors en mesure de les réinstaller rapidement et de les utiliser.

☑ J'utilise des logiciels de rechange. __
Pourquoi? Tout simplement parce qu'ils sont moins populaires. Lors d'une attaque de grande envergure, les logiciels malveillants doivent pouvoir infiltrer le plus d'ordinateurs possible. Ils cibleront alors un logiciel populaire, installé sur la majorité des ordinateurs, et l'utiliseront comme porte d'entrée en exploitant l'une de ses failles.

En possédant des logiciels moins connus, souvent gratuits et en plus, très efficaces, on réduit le risque d'attaque.

☑ **Bonnes habitudes et attitudes... avec mon courriel**

☑ Si j'utilise un service de courriel gratuit, je choisis un bon mot de passe

☑ Je n'ouvre jamais une pièce jointe à un courriel, sauf si je suis sûr à 110 % que le courriel provient d'une source sûre. __
Cette règle a une exception : lorsque la pièce jointe en question possède l'extension (les trois petits caractères après le nom d'un fichier) .EXE, .CMD, .BAT, .ZIP ou .RAR, il ne faut **jamais** l'ouvrir.

Il faut également être très vigilant avec les autres pièces jointes (document Word, document PowerPoint, images, etc.), car elles pourraient permettre l'infiltration de logiciels malveillants.

☑ Si je reçois un courriel de ma banque ou d'une institution financière contenant un hyperlien, je ne clique pas sur l'hyperlien et je supprime le courriel. __
Il est presque sûr qu'il s'agit d'un courriel d'hameçonnage (une tromperie). N'oubliez pas, les banques et autres institutions financières n'enverront **jamais** de courriel à leurs clients pour **solliciter** de l'information (avec un hyperlien ou avec un formulaire). Si elles écrivent à leurs clients, c'est pour leur transmettre un simple message d'information.

☑ Si je reçois n'importe quel type de courriel contenant un hyperlien (une carte de voeux, un avis, etc.), je ne clique pas sur l'hyperlien et suis extrêmement vigilant. __
L'hyperlien pourrait mener vers un site factice cherchant à voler vos renseignements personnels. Ou encore, il pourrait activer le téléchargement de logiciels malveillants.

Pour en savoir plus, cliquez sur « Menaces », puis sur « Hameçonnage ».

☑ Pour profiter des plaisirs du Web, j'utilise plusieurs adresses courriel dédiées. __
Il existe plusieurs services de courriel Web gratuits (Hotmail, Gmail, Yahoo, etc.), utilisez-les!

Utiliser plusieurs adresses courriel (au lieu d'une seule) est excellent pour réduire la quantité de pourriels reçue et limiter la propagation de votre adresse courriel « officielle ».

Voici quelques exemples : créez une adresse exclusive à visites sur ses sites de réseautage social (ex. : jaimelesreseauxsociaux@hotmail.com), une pour vos achats en ligne (ex. : joelemagasineur@gmail.com), etc.

☑ Si je crois avoir reçu un canular, je fais les vérifications nécessaires auprès de HoaxKiller.fr et de HoaxBuster.com.

☑ Je ne suis pas dans l'obligation de faire suivre une chaîne de courriels. __
Certains courriels demandent aux récipiendaires de faire suivre le message et de l'envoyer à 10, 15 ou 30 personnes, sans quoi de fâcheuses conséquences pourraient survenir (malheur, culpabilité, fermeture d'un compte courriel, etc.). Ces messages sont des canulars. Évitez de les transférer à vos contacts.

Pour en savoir plus, cliquez sur « Menaces », puis sur « Canular ».

☑ **Bonnes habitudes et attitudes... sur le site de ma banque**

☑ Je n'ajoute pas le site de votre banque à mes favoris. __
Pourquoi? Si un pirate réussit à infiltrer votre ordinateur, vous ne voulez tout de même pas le prendre

par la main et le guider vers le site de votre banque, n'est-ce pas?

☑ Pour accéder au site de ma banque, je tape son adresse dans la barre d'adresse au lieu d'utiliser un moteur de recherche. __
Pourquoi? Si une faille existe dans le moteur de recherche en question, elle pourrait être exploitée. Par exemple, s'il y a eu une telle manipulation malicieuse, l'adresse du site de votre banque figurant parmi les résultats de recherche pourrait être redirigée vers un site factice.

Il est évident que si vous ne connaissez pas l'adresse d'un site, vous pouvez utiliser un moteur de recherche. Toutefois, si vous souhaitez accéder au site de votre banque, priorisez l'usage de la barre d'adresse à celui d'un moteur de recherche.

☑ Je m'assure que la page où je dois entrer mes données confidentielles (numéro de compte, mot de passe, ou autres) est **sécurisée**. __
L'adresse URL de cette page doit commencer par « **https://...** ».

☑ J'utilise un bon mot de passe, fort et complexe.

☑ Avant d'entamer ma navigation, je démarre la navigation privée. Une fois ce mode activé, le navigateur ne sauvegardera pas l'historique de ma navigation, ne conservera aucun témoin ni fichier temporaire et n'enregistrera pas mes recherches. __
La navigation privée est une nouvelle fonctionnalité dans les navigateurs Mozilla Firefox et Internet Explorer. Pour la démarrer dans Mozilla Firefox, cliquez sur le menu « Outils », puis sur « Commencer la navigation privée ».

☑ Lorsque j'ai terminé, je ferme ma session en cliquant sur le lien à cet effet.

☑ Si je n'ai pas démarré de navigation privée, je vide le contenu de la mémoire cache et je supprime l'historique de navigation une fois ma session terminée. __
La mémoire stocke contient des fichiers qui pourraient contenir des traces de vos renseignements confidentiels.

Pour posséder à cette suppression dans Mozilla Firefox, cliquez sur le menu « Outils », puis sur « Supprimer l'historique récent ».

☑ Une fois mon navigateur fermé, je passe petit coup de balai avec un logiciel « de ménage ». __
Pourquoi? Pour éviter de laisser quelques traces menant vers le site de votre banque... ou vers vos renseignements confidentiels.

Tout ça peut paraître un peu exagéré, mais on n'est jamais trop prudent avec son argent. Vous ne laisseriez aucune trace de vos relevés bancaires dans votre bac à recyclage, n'est-ce pas? Alors n'en laissez pas plus dans votre ordinateur.

☑ **Bonnes habitudes et attitudes... si j'utilise un logiciel de pair-à-pair (*P2P*)**

☑ Je suis conscient que dès que j'**installe** un logiciel de pair-à-pair, je cours des risques. __
Des espiogiciels et des logiciels publicitaires, pour ne nommer que ceux-là, peuvent être greffés au logiciel de pair-à-pair. Par conséquent, ils s'installeront en même temps que le fameux logiciel de partage.

☑ Je suis conscient que dès que j'**utilise** un logiciel de pair-à-pair, je suis encore plus à risque. __
Les logiciels de pair-à-pair ouvrent votre ordinateur un réseau de partage où rien n'est sécuritaire. Quelqu'un, quelque part, pourrait décider de vous envoyer un logiciel malveillant par un port précis, non sécurisé, et malheureusement ouvert par le logiciel de pair-à-pair. Ou encore, un ver informatique pourrait être à l'oeuvre et utiliser un autre port non sécurisé pour circuler d'un ordinateur à l'autre... et aboutir sur le vôtre.

Et ce ne sont là que quelques exemples de problèmes occasionnés par ce type de logiciel.

- ☑ Surtout, je n'oublie pas qu'en plus d'être potentiellement **illégal**, c'est **dangereux**. __
  Le logiciel en soi n'est pas illégal, mais il véhicule bon nombre de fichiers illégaux et tout internaute pris à les télécharger ou à les transférer commet un acte illégal. Cependant, il n'y a aucun doutes sur sa dangerosité; utiliser un tel logiciel est très risqué.

☑ **Bonnes habitudes et attitudes... sur les sites de réseautage social**

Vous êtes parmi les 500 millions d'utilisateurs de Facebook? Pour plus de détails, cliquez ici.

- ☑ Sur le site de réseautage, si je reçois un message contenant un hyperlien (un courriel ou tout autre type de message), je ne clique pas sur l'hyperlien, même s'il est très tentant de le faire. __
  Il peut en effet s'agir d'un message d'hameçonnage. L'hyperlien pourrait vous mener vers un site factice cherchant à voler vos renseignements personnels, ou il pourrait activer le téléchargement de logiciels malveillants.
- ☑ Je gère mon profil et porte une attention particulière à la confidentialité de mes renseignements. __
  Les sites de réseautage social offrent, à la base, un minimum de protection des renseignements confidentiels. Pour une protection accrue, il faut repérer la page où se trouvent les paramètres de confidentialité et les gérer de manière plutôt « serrée ».

  Il faut cependant garder en mémoire que la « plus meilleure des protections » est d'utiliser ces sites avec jugement et discernement.
- ☑ Je limite au maximum l'information personnelle que j'y affiche. __
  Il n'est pas nécessaire d'afficher tout votre *pedigree*. N'oubliez pas, tout ce que vous choisissez de montrer pourra être vu et réutilisé par d'autres personnes qui ne font pas nécessairement partie de votre réseau d'« amis ».

  Certains sites de réseautage offrent des paramètres de confidentialité, mais la meilleure sécurité est encore de ne pas tout montrer. Un vol d'identité est si vite arrivé...
- ☑ Je limite le nombre de photos et je choisis celles que j'affiche. __
  Il n'est pas nécessaire d'afficher un véritable diaporama de votre portrait; quelques photos suffisent. N'offrez pas tout le nécessaire pour trafiquer et utiliser frauduleusement votre image. Vous avez une photo de vous faisant une grimace ou portant des lunettes de soleil? Elle sera parfaite!

☑ **Bonnes habitudes et attitudes... *lors de ma navigation***

- ☑ Je fais attention aux sites que je visite. S'ils sont illégaux, il y a de fortes chances qu'ils me créent des ennuis.
- ☑ Je fais encore plus attention aux sites que je visite. S'ils servent un objectif lubrique, il y a de fortes chances que je sois bombardé de publicités au charme douteux.

☑ **Bonnes habitudes et attitudes... avec la messagerie instantanée**

- ☑ J'utilise un logiciel autre que MSN Messenger/Windows Live Messenger.
  Besoin d'une solution de rechange? Essayez aMSN ou Trillian. __
  Pourquoi? Tout simplement parce qu'ils sont moins populaires que leur égal de Microsoft. De ce fait, ils seront moins ciblés par des attaques de grande envergure visant à infecter le plus d'ordinateurs possibles.
- ☑ Si je prévois quitter mon ordinateur pour plus d'une demi-heure, je quitte également mon logiciel de messagerie instantanée. __

Dès que le logiciel est ouvert, il est une porte d'entrée dans votre ordinateur.

Si vous quittiez votre domicile pour plus d'une heure, vous ne laisseriez pas la porte grande ouverte, n'est-ce pas? C'est la même chose avec un logiciel de messagerie instantanée. Si vous n'êtes pas devant votre ordinateur, quittez le logiciel et « fermez la porte ». Après tout, si l'un de vos contacts doit absolument vous parler, il pourra vous envoyer un courriel.

Donnez-moi ma liste Je recommence

--> Le site L'indispensable pour Internet a servi d'inspiration lors de la création de cette liste.

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Liste personnalisée de Annie

Bonnes habitudes et attitudes... avec mon ordinateur >>

- Je garde en mémoire que ma vigilance est de mise, car je suis responsable de ma sécurité et je suis impliqué dans celle de mon entourage.
- Je **prends le temps** d'apprendre comment fonctionne mon ordinateur.
- Je m'assure que mon système d'exploitation est à jour.
- Je fais régulièrement des sauvegardes (*backups*) de mes fichiers importants.
- Si j'éprouve une difficulté, je **ne panique pas** et je fais preuve de **patience**.

Bonnes habitudes et attitudes... avec mes logiciels >>

- Mon **pare-feu** est activé et bien paramétré.
- Mon **logiciel antivirus** est bien activé.
- Je scanne mon ordinateur avec mon logiciel antivirus au moins deux fois par mois.
- Une fois par semaine, je mets à jour les **signatures d'infection** de mon logiciel antivirus.
- J'ai installé **au moins deux logiciels antiespiogiciels**.
- Je scanne mon ordinateur avec chaque logiciel antiespiogiciel au moins une fois par semaine.
- Une fois par semaine, je mets à jour les signatures d'infection de chaque logiciel antiespiogiciel.
- J'ai une protection antiespiogicielle en temps réel et je m'assure qu'elle est activée.
- J'ai installé un logiciel « de ménage » et je l'utilise une fois par semaine.
- Je mets mon navigateur à jour lorsque nécessaire (par exemple, à l'affichage d'un avis de mise à jour.
- J'ai créé un cédérom de sécurité contenant les fichiers d'installation de tous les logiciels de sécurité installés sur mon ordinateur.
- J'utilise des **logiciels de rechange**.

Bonnes habitudes et attitudes... avec mon courriel >>

- J'utilise un bon mot de passe pour mon compte courriel.

- Pièce jointe : je ne l'ouvre pas sauf si je sais, à 110 %, qu'elle provient d'une source sûre. Si elle possède une extension .EXE, .CMD, .BAT, .ZIP ou .RAR, je ne l'ouvre pas.
- Courriel de ma banque ou d'une institution financière contenant un hyperlien : je ne clique pas sur l'hyperlien et je supprime le courriel.
- Courriel de n'importe quel type **contenant un hyperlien** : je ne clique pas sur l'hyperlien et suis extrêmement vigilant.
- Pour profiter des plaisirs du Web, j'utilise plusieurs adresses courriel dédiées.
- Canular : je fais les vérifications nécessaires auprès de HoaxKiller.fr et de Hoaxbuster.com.
- Je ne suis pas dans l'obligation de faire suivre une chaîne de courriels.

Bonnes habitudes et attitudes... sur le site de ma banque >>

- Le site de ma banque ne fait pas partie de la liste de mes favoris.
- Pour accéder au site de ma banque, je tape son adresse dans la **barre d'adresse**.
- La page où j'entre des données confidentielles est sécurisée : son adresse URL commence par « https://... ».
- J'utilise un bon mot de passe, fort et complexe.
- Avant de naviguer sur le site de ma banque, je démarre la navigation privée.
- Lorsque j'ai terminé, je ferme ma session en cliquant sur le lien à cet effet.
- Si je n'ai pas démarré de navigation privée : une fois la session fermée, je n'oublie pas de vider le contenu de la mémoire cache et de supprimer l'historique de navigation.
- Une fois le navigateur fermé, j'utilise le logiciel « de ménage ».

Bonnes habitudes et attitudes... si j'utilise un logiciel de pair-à-pair (*peer-to-peer*) >>

- Je sais que dès que j'installe ce logiciel, je suis à risque.
- Je sais que dès que j'utilise ce logiciel, je suis encore plus à risque.
- Je sais que dès qu'en plus d'être potentiellement **illégal**, c'est **dangereux**.

Bonnes habitudes et attitudes... sur les sites de réseautage social >>

- Sur le site de réseautage, si je reçois un message contenant un hyperlien, je ne clique pas dessus, **même s'il est très tenant de le faire**.
- Je gère mon profil et je porte une attention particulière à la confidentialité de mes renseignements.
- Je me protège contre le vol d'identité et je limite au maximum l'information personnelle que j'affiche.
- Je me protège contre le vol d'identité et je limite le nombre de photos affichées.

Bonnes habitudes et attitudes... lors de ma navigation >>

- Je me tiens loin des sites illégaux.
- Je me tiens loin des sites à caractère pornographique.

Bonnes habitudes et attitudes... avec la messagerie instantanée >>

- J'utilise un logiciel autre que MSN Messenger/Windows live Messenger. Exemples : aMSN ou Trillian.
- Dès que je quitte mon ordinateur pour plus d'une demi-heure, je quitte également mon logiciel de messagerie instantanée.

Moi, Annie, m'engage à respecter solennellement les bonnes habitudes et attitudes indiquées ci-haut afin d'assurer ma propre sécurité, et celle de mes contacts, sur Internet.

_____

Annie

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

FAITS DIVERS

La vie privée, le réseau Internet dans son ensemble et le populaire système d'exploitation Windows sont trois sujets qui touchent de près ou de loin à la sécurité Internet.

Que ce soit dans les médias ou au cours d'une discussion, l'un de ces faits divers peut surgir et susciter différents questionnements chez les internautes :

- « Est-ce que mon mot de passe est sécuritaire? »;
- « Être sur Facebook, est-ce risqué? »;
- « Un *botnet*, qu'est-ce que c'est? »;
- « Est-ce que je sais vraiment ce qu'est un *hacker*? »;
- « Est-ce que les mises à jour de Windows s'effectuent automatiquement sur mon ordinateur? »;
- « En quoi la restauration du système peut-elle m'être utile? »;
- Et bien plus encore.

Que ce soit pour répondre à vos questions, pour enrichir vos connaissances ou pour optimiser votre expérience, consultez les articles de faits divers et élargissez vos horizons.

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet
Maîtrise en études françaises cheminement communication et langages
Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Bien choisir un mot de passe

1. Les mots de passe et la piraterie

L'utilisation d'un mot de passe est maintenant chose commune. Chaque mot de passe permet d'ouvrir une porte la vie virtuelle d'un internaute et par le fait même, sur une foule de renseignements personnels. Étant donné la sensibilité de ces renseignements, un surcroît de sécurité s'impose pour tenir à distance les pirates et autres malfrats binaires, et cela commence par la création d'un mot de passe **fort** et **complexe**.

Les internautes d'aujourd'hui doivent composer avec plusieurs mots de passe, ce qui les incite parfois à choisir des options simples et faciles à retenir. Bien que ce choix avantage l'usager en lui évitant d'avoir à faire turbiner sa mémoire, il comporte de grands risques, car ses précieux mots de passe sont alors à la portée des pirates.

Ces derniers peuvent utiliser différentes techniques pour obtenir un mot de passe :

- **l'attaque par dictionnaire** : utiliser une application qui testera tous les mots que l'on trouve dans les dictionnaires de plusieurs langues, ainsi que les variations les plus populaires (par exemple, les mots dont la lettre « e » a été changée pour le chiffre « 3 »).
- **l'attaque par force brute :** utiliser une application qui tentera toutes les combinaisons de caractères possibles. De nos jours, les pirates peuvent employer un *botnet* lors d'une telle attaque, ce qui leur permet d'obtenir des résultats en très peu de temps (l'application peut tester des milliers de mots de passe à la seconde).
- **la fraude psychologique :** manipuler l'utilisateur pour qu'il remette son mot de passe de lui-même, par exemple lors d'une attaque par hameçonnage.
- **les logiciels malveillants :** les utiliser pour surveiller les activités des internautes et recueillir les renseignements pertinents, dont les mots de passe. L'enregistreur de frappe et le cheval de Troie, pour ne nommer que ceux-là, peuvent suffire à la tâche.
- **le vol :** plusieurs utilisateurs inscrivent leurs mots de passe sur un morceau de papier (caché parfois sous le clavier) ou dans un fichier texte sur leur ordinateur. Ils peuvent alors être volés

facilement.

ATTENTION

Si vous utilisez souvent votre ordinateur dans des lieux publics, soyez doublement vigilant. Un individu pourrait voler un mot de passe en observant « par-dessus votre épaule » les touches que vous tapez sur votre clavier. C'est ce qu'on appelle le *shoulder surfing*.

<< Retour

2. Les caractéristiques d'un bon mot de passe

Plus un mot de passe est sécuritaire, plus les pirates auront de la difficulté à l'obtenir. Alors, un bon mot de passe doit :

- **être long :** privilégiez l'utilisation d'au moins huit (8) caractères.
- **être diversifié :** mélangez les lettres minuscules et majuscules, les chiffres et les caractères spéciaux (#@!%?).
- **ne pas être un mot du dictionnaire :** oubliez les mots simples. Utilisez une combinaison de mots ou une phrase.
- **ne pas être issu de votre vie intime :** oubliez le nom de votre chien ou de votre enfant, la date de votre mariage ou celle de votre naissance. Ces mots de passe peuvent être devinés trop facilement.

Exemples :

Mauvais mots de passe :	Bons mots de passe :
○ amour	○ G1B#Nmotde(PASSE)
○ Frimousse	○ M#nCHAR(gris)478
○ Alic3	○ VAcanCeS1986(mer)

ATTENTION

Si vous craignez d'**oublier** votre mot de passe, inscrivez sur un bout de papier des indices servant à raviver votre mémoire, ou encore mieux, utilisez un logiciel de gestion des mots de passe.

La complexité du mot de passe créé doit aller de pair avec la sensibilité des données protégées. Le mot de passe d'un compte bancaire doit donc être plus sécuritaire que celui d'un compte personnel dans un forum de discussion. Cependant, peu importe le contexte du mot de passe, il doit posséder les caractéristiques énumérées ci-haut.

<< Retour

3. La modification du mot de passe

Une fois le mot de passe créé, chaque internaute doit savoir qu'il devra le modifier, mais pas trop souvent. Auparavant, il était conseillé de le changer fréquemment et cela comporte des inconvénients :

- il est facile de l'oublier;
- on choisit un mot de passe simple, justement pour éviter les risques d'oubli.

Ce dernier inconvénient est de taille, car on le sait, plus un mot de passe est simple, moins il est sécuritaire. Il est alors préférable de choisir un bon mot de passe et de le conserver plus longtemps. Mais il faut tout de même le changer! Garder le même mot de passe sur une trop longue période n'est pas souhaitable.

Il est conseillé de le modifier **deux fois par année**, par exemple à Noël et au Noël des campeurs, lors du changement des pneus sur une voiture, lors du changement d'heure, etc. Il faut choisir ses propres repères annuels et surtout, il faut les respecter.

IMPORTANT

Il est important de ne pas utiliser le même mot de passe pour plusieurs accès.

<< Retour

4. Sources documentaires

- Get Safe Online (anglais)
- Je protège mon identité sur Internet
- Wikipédia (français)

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Facebook

1. Qu'est-ce que Facebook?

Facebook est un site de réseautage social comprenant plus de 500 millions de membres d'un peu partout dans le monde. Sa popularité est indéniable et elle touche plusieurs générations d'internautes.

Facebook offre à ses membres la possibilité de se créer une page de profil et ensuite, d'entrer en contact avec des amis, tout ça gratuitement (du moins, en apparence). En effet, ce site est une formidable plateforme publicitaire pour les annonceurs.

<< Retour

2. Les renseignements des membres

Toute information divulguée sur Facebook peut être utilisée pour dresser un profil d'internaute à des fins de ciblage comportemental. De la publicité personnalisée est alors affichée dans les espaces à cet effet sur le site.

Et ça peut aller encore plus loin... Les membres sont invités à fournir beaucoup de renseignements, dont plusieurs ont un caractère confidentiel. Pris individuellement, un nom, un prénom ou une date de naissance sont presque inoffensifs. Mais une fois jumelés, ces renseignements deviennent un identifiant unique. Le risque de vol d'identité vient alors de grimper d'un cran. Si un individu affiche en plus son lieu de travail, son adresse postale, son adresse courriel, son numéro de téléphone, plusieurs photos de lui, etc., il remet toute l'information nécessaire pour faciliter le vol d'identité.

ATTENTION

Il existe un véritable marché noir des identités (en ligne et hors ligne). Certains pirates se spécialisent dans la recherche de renseignements sur des individus afin de bâtir des profils identitaires, pour ensuite les vendre. Plus un profil sera « garni », plus il sera vendu à fort prix.

Des sites comme Facebook deviennent alors une mine d'or pour ces pirates. Bon nombre de

membres n'ont aucun contrôle sur leur liste d'amis et ne protègent pas leur profil. De tels agissements facilitent la tâche des pirates, puisqu'ils peuvent facilement obtenir des renseignements dont ils ont besoin.

Soit dit en passant, bon nombre de pirates peuvent obtenir de l'information hors ligne, par exemple en téléphonant à un individu, en se faisant passer pour un professionnel quelconque et en lui soutirant des renseignements.

<< Retour

3. Les risques et les précautions

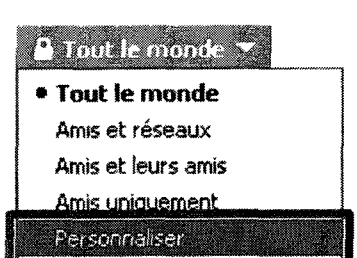
Malgré toutes les mises en garde, la popularité de Facebook ne décline pas. Il faut alors rappeler aux internautes qu'il s'agit d'un **site risqué** où la vigilance est de mise en tout temps.

Voici donc quelques conseils à mettre en application pour **se protéger sur Facebook** :

- **Adresse courriel :** Créez une adresse courriel exclusive à Facebook. De cette manière, si vous décidez d'abandonner le site, vous n'aurez qu'à abandonner l'adresse courriel et vous ne serez plus sollicité.
- **Mot de passe :** Choisissez un mot de passe fort et complexe.
- **Confidentialité :** Gérez vos paramètres de confidentialité. Assurez-vous entre autres de :
  - limiter l'accès à votre profil (dans la catégorie Profil);
  - contrôler l'accès à vos coordonnées (dans la catégorie Coordonnées);
  - bloquer le partage de vos données personnelles (dans la catégorie Applications et sites Web);
  - ajuster les paramètres de recherche (dans la catégorie Recherche).

CULTURE GÉNÉRALE

Sachez que vous pouvez personnaliser l'accès à vos renseignements d'une manière très précise. Par exemple, vous pouvez permettre à certains individus de voir vos photos, alors que d'autres ne le pourront pas. Il suffit de bâtir des listes d'amis et de choisir la bonne liste (en cliquant sur Personnaliser) lors du paramétrage des options de confidentialité.



- **Renseignements** :
  - N'enregistrez pas les renseignements suivants dans votre profil :
    - Votre vraie date de naissance (distancez-la d'un jour ou deux);
    - Adresse courriel;
    - Adresse postale;
    - Numéro(s) de téléphone (fixe et cellulaire);
    - Lieu de travail.
  - Gardez un contrôle serré sur ces renseignements :
    - Nom et prénom (n'hésitez à utiliser un surnom);
    - Situation amoureuse;
    - Nom et prénom du conjoint ou de la conjointe (c'est une bonne ressource pour deviner un mot de passe);
    - Villes actuelle et d'origine;
    - Membres de la famille;
    - Formation.
  - N'en dites pas trop sur vous, restez-en au strict minimum. Toute information affichée sur le Web devient difficile, voire impossible à contrôler. Plus vous en donnez, plus il est facile de perdre le contrôle.
- **Photos :**
  - Limitez le nombre de photos affichées.
  - Laissez tomber les photos de vous sous tous vos angles, car vous offrez alors tout le nécessaire pour trafiquer et utiliser frauduleusement votre image. Vous avez une photo de vous faisant une grimace ou portant des lunettes de soleil? Elle sera parfaite.
- **Demandes d'amitié :** Ne vous sentez pas obligé d'accepter toutes les demandes d'amitié. Si vous ne connaissez pas la personne, refusez.
- **Liste d'amis :** Gardez le contrôle sur votre liste d'amis. Plus vous en avez, plus il est difficile de la gérer. Par exemple, vous pourriez publier un commentaire désobligeant sur votre travail en ayant oublié que bon nombre de vos collègues (et votre patron) sont vos amis Facebook...
- **Communication :** Si vous devez envoyer des renseignements sensibles à un contact (comme une adresse, un numéro de téléphone, ou même la date d'un rendez-vous), ne les inscrivez pas sur son babillard, privilégiez plutôt l'envoi d'un message privé.
- **Applications :** N'installez pas d'applications superflues, car elles peuvent télécharger des logiciels malveillants sur votre ordinateur.
- **Courriels :** Faites très attention aux pourriels et aux courriels d'hameçonnage créés à partir des courriels de Facebook. Ils peuvent vous mener vers des sites factices potentiellement dangereux.

<< Retour

4. Sources documentaires

- Facebook - Statistics (anglais)
- Get Safe Online (anglais)
- Je protège mon identité sur Internet
- Wikipédia (français)

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

Protéger sa vie privée sur Internet

1. Une vie privée connectée

Internet est un immense réseau rassemblant des centaines de millions d'individus. Malgré les apparences, il n'a rien de privé : dès que vous êtes connecté, votre vie virtuelle devient accessible.

Pour protéger sa vie privée sur Internet, une judicieuse combinaison de précautions logicielles et comportementales est nécessaire.

<< Retour

2. Les logiciels

Voici les logiciels essentiels pour vous aider à **protéger votre vie privée**. Pour obtenir des suggestions de gratuiciels à télécharger, cliquez sur le lien du logiciel concerné.

- Un pare-feu;
- Un logiciel antivirus;
- Au moins deux logiciels antiespiogiciels;
- Un logiciel « de ménage » :
- Un navigateur autre qu'Internet Explorer;
- Si vous avez besoin d'un logiciel de courriel, choisissez-en un qui contient un filtre antipourriel.

<< Retour

3. Les comportements

Tous ces logiciels peuvent devenir inefficaces si l'internaute qui les utilise n'adopte pas les comportements adéquats. Voici quelques règles à suivre pour que ces logiciels contribuent à la

protection de votre vie privée :

- Activez votre pare-feu et votre logiciel antivirus en tout temps.
- Apprenez à mettre à jour régulièrement les logiciels suivants :
  - Système d'exploitation;
  - Navigateur;
  - Logiciel antivirus (les signatures d'infection doivent être à jour);
  - Logiciels antiespiogiciels (les signatures d'infection doivent être à jour).
- Paramétrez adéquatement votre pare-feu, selon vos besoins. Lors de votre utilisation d'Internet, le pare-feu fera apparaître des boîtes de dialogue qui se chargeront de ce paramétrage en vous demandant si vous autorisez (ou refusez) le transfert de données effectué par un logiciel ou un service. Votre décision sera alors enregistrée sous forme de règle et votre pare-feu la respectera à l'avenir.
  - Si vous avez besoin d'aide, n'hésitez pas à consulter les rubriques d'aide de votre pare-feu. Contrairement à ce que l'on peut croire, cette fonctionnalité renferme une foule de renseignements utiles.
- Scannez votre ordinateur avec le logiciel antivirus au moins deux fois par mois.
- Scannez votre ordinateur avec chaque logiciel antiespiogiciel au moins une fois par semaine.
- Choisissez des mots de passe forts et complexes
- Scannez votre ordinateur et votre base de registre avec le logiciel « de ménage » régulièrement, une fois par semaine si nécessaire.

Certaines habitudes relèvent toutefois du « Code 18 », c'est-à-dire 18 pouces derrière l'écran.

Comme il est parfois difficile de se rappeler de tous les bons comportements à adopter, créez une liste personnalisée de bonnes habitudes et attitudes, imprimez-la et utilisez-la comme aide-mémoire.

- Liste personnalisée de bonnes habitudes et attitudes

<< Retour

4. Sources documentaires

- Get Safe Online (anglais)
- Wikipédia (français)

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a eté conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

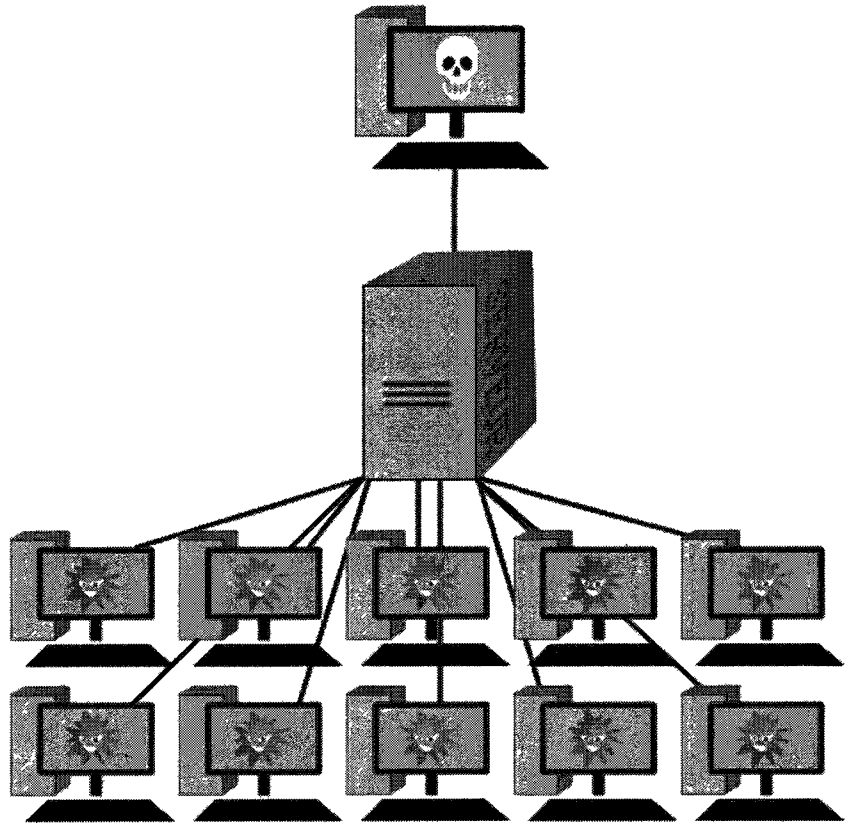
Utiliser Internet de manière intelligente et sécuritaire

Botnet

1. Une description

Le *botnet* (ou réseau de zombies) est, comme son nom le suppose, un réseau d'ordinateurs zombies contrôlé à distance par un pirate. Il permet au pirate d'obtenir une superpuissance dont il pourra se servir pour commettre différents actes : envoi massif de pourriels ou de courriels d'hameçonnage, attaque contre un site Web, attaque par force brute pour obtenir un ou des mots de passe, etc.

Chaque ordinateur qui compose le *botnet* a préalablement été infecté par un logiciel malveillant spécialement conçu pour le transformer en zombie. Il est ensuite rallié de force à l'armée du *botnet*, bien souvent à l'insu de son utilisateur. Il tombe finalement sous le contrôle d'un pirate qui « gère » l'armée au complet grâce à un serveur *bot*.



<< Retour

2. Le fonctionnement

Au commencement, il y a un pirate vivant une quelconque frustration, souhaitant faire un peu d'argent ou désirant mettre ses talents à l'épreuve. Pour arriver à ses fins, il sait pertinemment que son unique ordinateur et sa seule connexion Internet ne suffiront pas, alors il entame la création de son armée.

Pour ce faire, il a recours à un logiciel malveillant (un ver informatique, un cheval de Troie, un espiogiciel, etc.) dont l'objectif est de transformer chaque ordinateur infecté en zombie. Il se charge ensuite de sa diffusion et peut employer divers moyens :

- créer un site Web infecté et utiliser un courriel d'hameçonnage pour appâter les internautes;
- pirater un moteur de recherche pour rediriger automatiquement des internautes vers un site piégé;
- exploiter une faille dans un logiciel populaire;
- s'introduire de force dans un réseau pour en infecter tous les ordinateurs;
- etc.

ATTENTION

Si votre ordinateur est protégé par un pare-feu, si vos logiciels sont à jour (système d'exploitation,

navigateur, logiciel de courriel, etc.) et si vos activités en ligne ne frôlent pas l'illégalité, le risque s'en trouve réduit.

Bref, il y a une panoplie de moyens pour permettre à un pirate d'infecter un ordinateur. Malheureusement, la quantité de réseaux et d'ordinateurs mal ou non sécurisés connectés à Internet est importante, ce qui facilite la propagation de logiciels malveillants.

Dès qu'un ordinateur devient un zombie, il se peut qu'un utilisateur peu alerte ne remarque rien du tout; au plus notera-t-il quelques ralentissements. Pourtant, sa connexion Internet pourra être exploitée au même stade que la puissance de son ordinateur (d'où les ralentissements). Certains logiciels malveillants peuvent même désactiver des mesures de sécurité (dont le logiciel antivirus) pour éviter d'être repérés.

Le logiciel malveillant à l'origine de l'infection est programmé pour avertir le pirate lorsqu'il est bien en place. Lorsque le pirate a reçu un nombre suffisant de signaux, il va de l'avant. Le *botnet* peut alors être utilisé par son propriétaire, ou encore être vendu ou loué.

CULTURE GÉNÉRALE

Parfois, il arrive que l'armée soit si volumineuse qu'un seul pirate, derrière un seul serveur *bot*, ne suffit plus à la tâche. Il doit alors requérir les services d'autres serveurs *bots*.

Les *botnets* peuvent contenir des centaines de milliers de zombies et l'un des plus impressionnants en ralliait 1,5 million. Il avait été conçu par des pirates allemands pour demander des rançons à des entreprises américaines, procéder à des vols d'identité et propager des espiogiciels.

Un pirate peut commettre toutes sortes d'actes avec un *botnet*[1] :

- Recruter d'autres ordinateurs pour agrandir le *botnet* actuel, ou en créer un autre, ce qui peut être payant lors d'une vente ou d'une location;
- Procéder à une attaque par saturation, par exemple contre un site Web ennemi ou contre le serveur d'un compétiteur;
- Installer massivement des logiciels publicitaires et (ou) des espiogiciels. Il arrive que des entreprises achètent et utilisent de tels *botnets* à des fins publicitaires, ce qui est désormais contraint par la loi (mais encore faut-il trouver les fautifs pour les punir);
- Faire des envois massifs de pourriels ou de courriels d'hameçonnage. Encore une fois, les espoirs lucratifs nourrissent ce type d'attaques;
- Stocker ou distribuer du matériel informatique illégal ou protégé par la propriété intellectuelle;
- Servir de levier pour demander une rançon à une entreprise, par exemple sous la menace d'une attaque (qui peut être très convaincante).
- Recueillir des données confidentielles en tous genres, que ce soit pour envoyer de la publicité ou procéder à un vol (d'argent ou d'identité);
- Etc.

Soit dit en passant, le *botnet* est l'outil idéal pour un pirate ne souhaitant pas se faire repérer, car il lui permet de se cacher derrière une armée. Si jamais le *botnet* est détecté par les autorités, ce

seront les zombies qui seront repérés en premier. Souvent, le délai nécessaire pour traverser ce mur de zombies est suffisamment long pour permettre au pirate de fermer son réseau et de camoufler toutes traces de ses actes. Ce sont alors les zombies qui accusent les coups, puisqu'ils sont complices du pirate. Et leurs utilisateurs, même s'ils ignorent tout de cette situation, sont à risque d'en faire les frais.

<< Retour

3. Des conséquences

Les conséquences des *botnets* sont très diversifiées pour les individus. D'abord, il y a celles du logiciel malveillant à l'origine de l'infection (ver informatique, cheval de Troie, espiogiciel, etc.). Ensuite, la participation au réseau a des effets sur l'ordinateur zombie et son utilisateur :

- L'ordinateur peut subir des ralentissements;
- L'exploitation de la bande passante peut ralentir, voire bloquer, le fonctionnement de la connexion Internet;
- Le logiciel antivirus (et autres mesures de sécurité) peut être désactivé à l'insu de l'utilisateur;
- L'utilisateur se retrouve dans une situation où il est complice d'un acte illégal, et ce, à son insu;
- Etc.

Les entreprises sont également à risque de subir d'importantes conséquences : lourdes pertes financières, écroulement du site Web, piratage du réseau, exploitation de la bande passante, etc. Ce n'est pas pour rien que de nombreuses entreprises victimes d'une attaque par *botnet* décident de poursuivre au criminel les pirates à leur origine (si elles arrivent à les trouver).

<< Retour

4. La prévention

Pour éviter qu'un ordinateur soit rallié de force à un *botnet,* il faut le protéger contre les logiciels malveillants qui se chargent de la « zombification ». Cette prévention doit être logicielle et comportementale.

Protection logicielle :

- Un logiciel antivirus activé en tout temps et dont les signatures d'infection sont à jour;
- Au moins deux logiciels antiespiogiciels dont les signatures d'infection sont à jour;
- Un pare-feu paramétré adéquatement.

Protection comportementale :

- Mettre les logiciels suivants à jour :
    - Logiciel antivirus (pour mettre les signatures d'infection à jour);

    - Logiciels antiespiogiciels (pour mettre les signatures d'infection à jour);
    - Système d'exploitation;
    - Navigateur;
    - Tout autre logiciel bénéficiant de correctifs de sécurité (téléchargés lors des mises à jour) : logiciel de courriel, logiciel de messagerie instantanée logiciel de lecture des PDF, lecteur de musique, suite bureautique, logiciel de graphisme, jeu, etc.
- Choisir des mots de passe forts et complexes;
- Éviter d'utiliser un logiciel de pair-à-pair et de faire des téléchargements à partir de sources non fiables;
- Faire preuve de vigilance.

<< Retour

5. La guérison

Si vous savez que votre ordinateur fait partie d'un *botnet*, voici ce que vous pouvez faire :

1. Installez un pare-feu, pour éviter que le problème ne prenne de l'ampleur.
2. Redémarrez votre ordinateur en mode sans échec.
3. Analysez votre ordinateur avec un logiciel antivirus.
   Supprimez les menaces détectées, s'il y en a.
4. Analysez votre ordinateur avec un logiciel antiespiogiciel .
   Supprimez les menaces détectées, s'il y en a.
5. Analysez votre ordinateur avec un deuxième logiciel antiespiogiciel.
   Supprimez les menaces détectées, s'il y en a.
6. Redémarrez votre ordinateur en mode Normal.

<< Retour

6. Sources documentaires

- Best Security Tips (anglais)
- Grand dictionnaire terminologique
- Techweb (anglais)
- Wikipédia (français)
- SCHILLER, Craig A. et Jim BINKLEY, David HARLEY, Gadi EVRON, Tony BRADLEY, Carsten WILLEMS, Michael CROSS. *Botnets : The Killer Web App*, [s.l.], Syngress Publishing, Inc., 2007, 464 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Fonctionnement du DNS (*Domain Name System*)

1. Une description

Le DNS (ou *Domain Name System*) est un système permettant d'établir un lien entre une adresse IP et un nom de domaine afin de diriger un internaute vers un site Web.

IMPORTANT

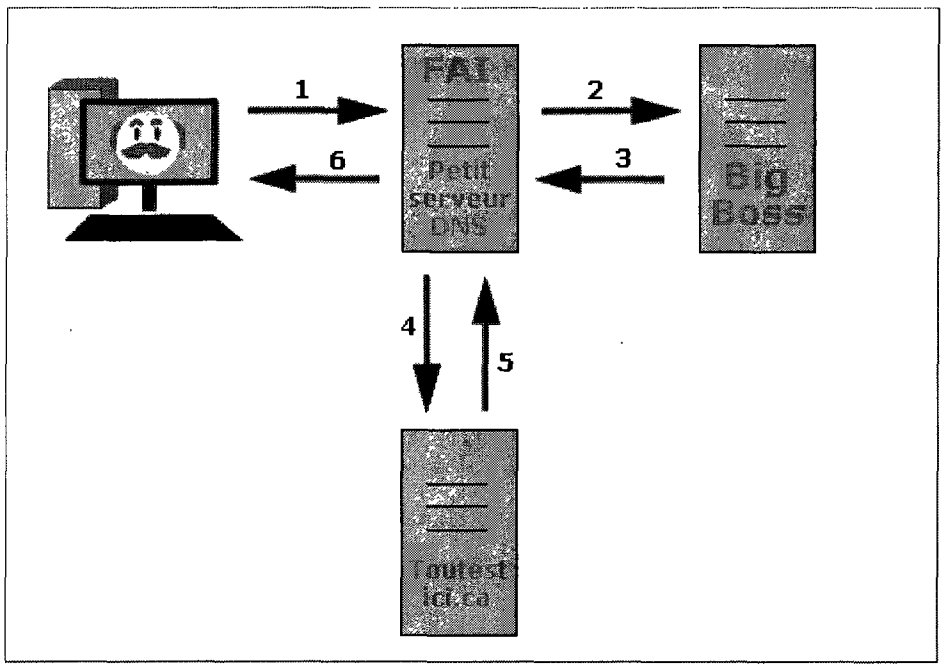
Il faut savoir que le DNS est un système et il implique deux choses : les serveurs DNS (côté serveur... c'est-à-dire du côté d'Internet) et le cache DNS (côté client... c'est-à-dire de votre côté, dans votre ordinateur).

Soit dit en passant, les serveurs DNS peuvent également posséder un cache DNS. Toutefois, toute mention « cache DNS » dans ce site fait référence au cache DNS du côté client.

<< Retour

2. Un exemple

Pour bien comprendre le fonctionnement du DNS, voici un exemple.



Roger veut accéder au site http://www.usherbrooke.ca. Il fait sa requête en tapant cette adresse URL dans la barre d'adresse de son navigateur.

La requête est immédiatement envoyée au serveur du FAI (**1**), qui part à la recherche de l'adresse IP du site en question. Pourquoi cherche-t-il l'adresse IP? Car le FAI ne parle que le numérique. L'adresse URL « http://www.usherbrooke.ca » ne lui dit rien, il a besoin de l'adresse IP correspondante pour afficher le site.

Il demande donc à son serveur DNS (« petit serveur DNS ») de trouver l'adresse IP correspondante. Petit serveur DNS va directement au sommet de la hiérarchie et demande au serveur racine du DNS (« big boss ») où il peut trouver l'adresse IP recherchée (**2**). Le big boss lui répond : « Va voir dans le serveur DNS "Toutestici.ca", tu y trouveras ce que tu cherches. » (**3**)

Petit serveur DNS entre donc en contact avec le serveur DNS « Toutestici.ca » (**4**), qui s'empresse de lui envoyer l'adresse IP correspondante (**5**). Petit serveur DNS remet donc ce renseignement au serveur du FAI, satisfait de comprendre enfin à quel site correspond l'adresse URL « http://www.usherbrooke ». Le serveur du FAI affiche alors le site Web dans le navigateur de Roger (**6**).

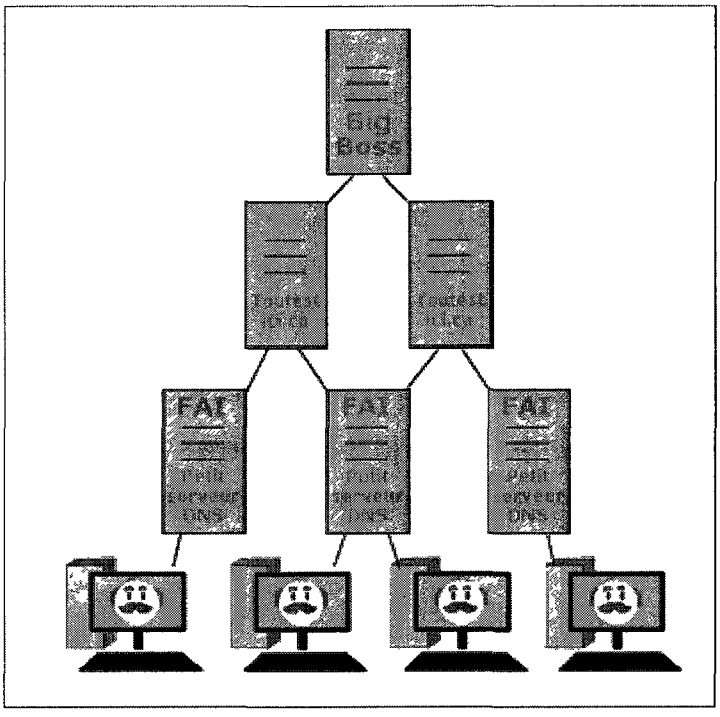
Tout ça bien sûr en une fraction de seconde. Et si plus tard Roger souhaite accéder de nouveau au site http://www.usherbrooke.ca, son système n'aura qu'à jeter un coup d'oeil au cache DNS de son ordinateur, où la conversion a été mise en mémoire.

<< Retour

3. La hiérarchie

Il est important de savoir que les serveurs DNS respectent une hiérarchie. Avec l'aide de l'exemple précédent, voici à quoi cette hiérarchie ressemble. Fait à noter, il existe une multitude de FAI et de

serveurs équivalents à « Toutestici.ca », mais il n'y a qu'un seul « big boss ».



<< Retour

4. Sources documentaires

- Wikipédia (français)
- Wikipedia (anglais)

<< Retour

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

indicateurs de sites factices

Vous avez des doutes sur la légitimité d'un site Web? Observez son adresse. Elle peut vous donner des indices pour découvrir si vous êtes sur un site factice ou non.

Quelques indicateurs et les exemples mentionnés ci-dessous sont tirés du site *Reasonable Anti-Phishing* (anglais).

- Si la page demande des renseignements (identification, formulaire, etc.), elle doit être sécurisée et commencer par « **https://...** ».

- L'adresse URL peut être inutilement longue et débuter par des chiffres et lettres inconnus. Par exemple,
  http://c-76-108-179-168.hsd1.fl.comcast.net/www.paypal.com/cgi-bin/webscr.php?cmd=_flow&session=60-sqeap_wwvhpmjul-dllc5oku8dzthcy4mf5lzvzxgdmvlhbsjcflcmuw&dispatch=5885d89092
  au lieu de
  https://www.paypal.com.

- L'adresse URL peut débuter par un nom différent de celui du site concerné.
  Par exemple,
  http://www.bestgifts.ro/https/PayPal-usercmdID12549JDk23_account-confirm/ au lieu de
  https://www.paypal.com.

- L'adresse URL peut débuter par une série de nombres inconnus.
  Par exemple,
  http://200.107.32.91/paypal/
  au lieu de
  https://www.paypal.com.

- L'orthographe du nom de domaine dans l'adresse URL est erronée.
  Par exemple,
  http://www.paypal.com
  au lieu de
  https://www.paypal.com

Sources documentaires

- Reasonable Anti-Phishing (anglais)
- Wikipédia (français)

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

pirates Internet

1. Des internautes parmi tant d'autres

Parmi la population internaute grandissante, tous n'ont pas d'honnêtes intentions au moment de leur utilisation d'Internet. Après tout, les différentes menaces circulant sur la toile sont aussi diversifiées que les individus à leur origine. Mais qui sont donc ces « auteurs » malintentionnés?

CULTURE GÉNÉRALE

Si seulement 0,5 % des 1,8 milliard d'internautes possède de mauvaises intentions, cela représente tout de même 900 000 personnes susceptibles de piraterie.

Tous on déjà entendu parler des *hackers*. Mais il faut savoir qu'ils ne sont pas seuls dans l'univers de la piraterie; il y a aussi les *crackers* et les *crashers*, bien plus redoutables.

<< Retour

2. Les *hackers*

Les ***hackers*** sont les premiers à avoir œuvré dans le domaine de l'attaque informatique, et ce, dès la fin des années 1970. Ils n'étaient alors qu'une poignée d'experts souhaitant :

- signaler, avec les preuves nécessaires à l'appui, des problèmes de sécurité informatique pouvant être exploités;
- tester leurs habiletés (par curiosité intellectuelle), sans toutefois causer de dommages.

Les *hackers* sont toujours présents de nos jours, mais ils servent un objectif qui va bien au-delà de la simple piraterie Internet. Ils se battent entre autres pour éviter toute mainmise propriétaire sur le réseau Internet et n'hésitent pas à dénoncer ceux qui, selon eux, l'exploitent pour générer de larges profits. « Ils se présentent donc comme des redresseurs de torts et ambitionnent de montrer les points faibles des réseaux et des systèmes informatiques[1]. »

Le terme *hacker* a acquis, dans les années 90, une connotation péjorative à cause d'une décision des autorités publiques françaises voulant que la traduction officielle du *hacking* soit le « piratage informatique ». Cependant, les vrais *hackers* sont loin d'être des pirates malfaisants comme le sont les *crackers* et les *crashers* en raison, entre autres, du fait qu'ils seraient portés à « travailler contre les vrais pirates ».

<< Retour

3. Les *crackers* et les *crashers*

En ce qui concerne les ***crackers*** et les ***crashers***, une confusion s'est établie et elle a comme origine la nature malveillante de ces deux catégories de pirates. Certains vont même jusqu'à les utiliser en tant que synonymes, mais il n'en est rien, leurs actions étant de natures très différentes. Les *crackers* cherchent à usurper ou à endommager, tandis que les *crashers* veulent causer des plantages (ou *crashs*).

CULTURE GÉNÉRALE

En raison de leur malveillance, on qualifie les *crackers* et les *crashers* de pirates « à chapeau noir » (*Black Hat*). À titre de comparaison, les *hackers* œuvrant contre la piraterie sont surnommés pirates « à chapeau blanc » (*White Hat*) et les modérés, travaillant parfois d'un côté, parfois de l'autre, sont les pirates « à chapeau gris » (*Grey Hat*).

À l'origine, le travail des ***crackers*** consistait à pirater le code des logiciels afin d'en « casser » les protections, ou encore à pénétrer des systèmes informatiques sans aucune permission. De nos jours, ils procèdent entre autres à des vols d'identités et à l'endommagement des infrastructures de systèmes informatiques, des portails Web ou des sites Web, tout en continuant de remplir leurs « tâches originales ».

Les ***crashers***, quant à eux, faisaient planter des systèmes informatiques lors de leurs débuts, et ce, par défi ou par plaisir. Aujourd'hui, cet objectif de plantage subsiste, mais il cible également les sites Web, les portails Web et les serveurs Internet.

Qu'en est-il de leurs compétences? Qu'ils soient *crackers* ou *crashers*, les pirates malfaisants n'ont pas tous la même expérience ni les mêmes habiletés. Il en résulte alors différents degrés de compétences.

- Il y a d'abord les ***script kiddies***, soit des débutants en informatique utilisant les outils disponibles sur Internet et conçus par des pirates plus performants. Ils n'ont pas nécessairement de connaissances très poussées en programmation, mais ils peuvent tout de même provoquer des dommages. Cependant, leur manque de connaissances et d'habileté facilite leur repérage et l'arrêt de leurs activités.
- Il y a ensuite les **intermédiaires**, qui ont les connaissances suffisantes pour causer de sérieux dégâts. Ils connaissent les rouages de l'informatique et des réseaux et surtout, ils savent comment les exploiter.
- Finalement, il y a les **experts**. Ils s'affairent habituellement au développement de plusieurs outils de piratage (entre autres ceux utilisés par les *script kiddies*) et de logiciels malveillants

(comme les virus et les vers informatiques). Ils sont également auteurs d'*exploits* et maîtrisent l'art de l'implantation de logiciels malveillants, tout comme celui de l'intrusion dans un serveur afin d'en prendre le contrôle.

QUESTION

« Qu'est-ce qu'un *exploit*? » Il s'agit d'un bout de code permettant de commettre une attaque. Plus précisément, un individu le conçoit pour profiter d'une faille dans un système d'exploitation ou dans un autre logiciel. Ensuite, il peut l'utiliser pour prendre le contrôle d'un ordinateur ou effectuer une attaque.

Bref, les pirates Internet ne sont pas tous issus du même gabarit; ils se distinguent par leurs actes, par leurs connaissances et par leurs compétences.

Ils ne sont pas tous des « êtres surdoués, très intelligents, mais extrêmement malicieux », certains ne sont que des novices à la recherche de sensations fortes. Ces « apprentis » peuvent être tout de même très dangereux, car la portée des dommages causés peut aller bien au-delà de ce à quoi ils s'attendaient (pensons au célèbre Mafiaboy). Un simple mauvais tour peut alors virer au drame.

<< Retour

4. Sources documentaires :

- Cyberpresse
- Le Devoir
- Internet World Stats (anglais)
- Wikipédia (français)
- Wikipedia (anglais)
- TRABELSI, Zouheir et Henri LY. *La sécurité sur Internet*, Paris, Hermès Science Publications, 2005, 254 p.
- BEAVER, Kevin. *Comment combattre les hackers pour les nuls*, coll. « Pour les Nuls », Paris, Éditions First Interactive, 2004, 423 p.

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises cheminement communication et langages

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Désinstaller un logiciel sous windows

1. Désinstaller un logiciel

Lorsque vient le temps de supprimer un logiciel, il est important de ne pas simplement sélectionner quelques fichiers et de les supprimer. Cette manière de procéder ne fait que désinstaller une partie du logiciel, empêche sa suppression « complète » et pourrait nuire au bon fonctionnement de certaines fonctions de Windows.

Il faut plutôt utiliser une fonctionnalité de Windows spécialement conçue à cet effet, ce qui permet une désinstallation efficace.

<< Retour

2. La désinstallation sous Windows XP

1. Cliquez sur le menu Démarrer;
2. Cliquez ensuite sur Panneau de configuration;
3. Double-cliquez sur l'icône « Ajout/Suppression de programmes »;
4. Sélectionnez le logiciel à désinstaller dans la liste;
5. Cliquez sur le bouton Désinstaller.

<< Retour

3. La désinstallation sous Windows Vista et Windows 7

1. Cliquez sur le menu Démarrer;
2. Cliquez ensuite sur Panneau de configuration;
3. Cliquez sur Programmes, puis sur Programmes et fonctionnalités;
4. Sélectionnez le logiciel à désinstaller dans la liste;

5. Cliquez sur le bouton Désinstaller.

<< Retour

4. Sources documentaires

- Aide et support de Microsoft
- Wikipédia (français)

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Gestion du pare-feu Windows

1. Un pare-feu qui évolue

Le pare-feu Windows est un dispositif logiciel de pare-feu inclus dans les systèmes d'exploitation Microsoft Windows XP (Service Packs 2 et 3), Windows Vista et Windows 7.

Les pare-feu, habituellement, peuvent filtrer les données qui entrent et qui sortent d'un ordinateur; ils agissent dans les deux sens. À l'inverse, le pare-feu de Windows XP agit dans un seul sens : il peut bloquer les intrusions, mais n'a aucun contrôle sur les données qui sortent de l'ordinateur. Cette situation peut être problématique si l'ordinateur est infecté par certains types de parasites comme les espiogiciels et les chevaux de Troie qui, une fois installés sur un ordinateur, vont « faire sortir » des données pour les envoyer à une tierce personne. Bref, le pare-feu de Windows XP n'est pas idéal, puisqu'il n'est pas efficace à 100 %. Il est alors préférable d'opter pour un autre pare-feu.

Cette problématique a été corrigée dans le pare-feu de Windows Vista/Windows 7. Il est désormais en mesure de filtrer les données entrantes et sortantes, ce qui le rend plus efficace que son prédécesseur.

Si un pare-feu autre que celui de Windows est utilisé, il est important de vérifier que le pare-feu de Windows et proprement désactivé, car un ordinateur ne doit posséder qu'un seul pare-feu (pour en savoir plus, consultez les Questions + réponses). Pour faire cette vérification, ou pour apporter des modifications, veillez à suivre la procédure ci-dessous qui correspond à votre système d'exploitation Windows.

<< Retour

2. La gestion du pare-feu sous Windows XP

1. Cliquez sur le bouton « Démarrer » dans le coin inférieur gauche de votre écran;
2. Cliquez ensuite sur le sous-menu « Panneau de configuration »;
3. Double-cliquez sur « Pare-feu Windows ». Une boîte de dialogue apparaîtra et vous pourrez

voir si le pare-feu Windows est activé et apporter des changements, si souhaité.

<< Retour

3. La gestion du pare-feu sous Windows Vista

1. Cliquez sur le bouton « Démarrer » dans le coin inférieur gauche de votre écran;
2. Dans le module de recherche, juste au-dessus du bouton « Démarrer », tapez « pare-feu »;
3. Cliquez ensuite sur « Pare-feu Windows ». Une boîte de dialogue apparaîtra et vous pourrez voir si le pare-feu Windows est activé et apporter des changements, si souhaité.

<< Retour

4. La gestion du pare-feu sous Windows 7

1. Cliquez sur le bouton « Démarrer » dans le coin inférieur gauche de votre écran;
2. Cliquez ensuite sur « Panneau de configuration »;
3. Dans la zone de recherche, tapez « pare-feu »;
4. Cliquez ensuite sur « Pare-feu Windows ». Une boîte de dialogue apparaîtra et vous pourrez voir si le pare-feu Windows est activé et apporter des changements, si souhaité.

<< Retour

5. Sources documentaires

- Aide et support de Microsoft
- Memoclic
- Softpedia (anglais)
- Wikipedia (anglais)

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en etudes françaises, cheminement comunication et langages

Universite de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Mises à jour de Windows

1. L'importance des mises à jour

Comme l'ensemble des logiciels, le système d'exploitation a des failles, parfois petites, parfois grandes. Pour que ces brèches soient « colmatées », il doit être régulièrement mis à jour.

Le système d'exploitation Windows propose un système de mise à jour appelé Windows Update. Habituellement, il est paramétré pour que les mises à jour s'installent automatiquement. Pour vous assurez que ce service s'exécute automatiquement, ou pour apporter des modifications, veillez à suivre la procédure ci-dessous qui correspond à votre système d'exploitation Windows.

<< Retour

2. Windows Update sous Windows XP

1. Cliquez sur le bouton « Démarrer » dans le coin inférieur gauche de votre écran;
2. Cliquez ensuite sur le sous-menu « Panneau de configuration »;
3. Doublez-cliquez sur l'icône « Centre de sécurité »;
4. Une boîte de dialogue apparaîtra. Dans la zone inférieure, vous verrez « Gérer les paramètres de sécurité pour : »;
5. Cliquez sur « Mises à jour automatiques ».

<< Retour

3. Windows Update sous Windows Vista

1. Cliquez sur le bouton « Démarrer » dans le coin inférieur gauche de votre écran, puis sur « Tous les programmes »;

2. Cliquez sur « Windows Update »;
3. Cliquez par la suite sur « Modifier les paramètres » dans le volet de gauche.

<< Retour

4. Windows Update sous Windows 7

1. Cliquez sur le bouton « Démarrer »;
2. Tapez « Update » dans la zone de recherche;
3. Cliquez sur « Windows Update »;
4. Cliquez par la suite sur « Modifier les paramètres » dans le volet de gauche.

<< Retour

5. Sources documentaires

- Grand dictionnaire terminologique
- Aide et support de Microsoft
- Wikipedia (anglais)
- Wikipédia (français)

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Mode sans échec

1. Une description

Le mode sans échec permet de démarrer un ordinateur avec un minimum de ressources logicielles. Il offre par conséquent moins de possibilités que le mode normal. Majoritairement utilisé en cas de problèmes, ce mode permet de détecter les incidents sans que l'ordinateur ne soit « brouillé » par des logiciels non essentiels à son fonctionnement ni par des logiciels malveillants.

<< Retour

2. Démarrer en mode sans échec sous Windows

Fait à noter, cette procédure est valide pour les systèmes Windows XP, Windows Vista et Windows 7.

1. Lors du démarrage de l'ordinateur, lorsque l'écran est noir juste avant l'apparition du logo de Windows, appuyez sur la touche F8 (plusieurs fois si nécessaire). *Si la touche F8 ne fonctionne pas, essayez la touche F5.*
2. Plusieurs choix s'offrent alors à vous. Choisissez l'option « Mode sans échec » et appuyez sur Entrée.
3. Vous verrez alors une série de lignes de code défilant sur un fond noir. C'est normal, soyez patient.
4. Vous verrez ensuite le bureau de Windows, mais avec un affichage plus sobre, une résolution sommaire et les mentions « Mode sans échec » au haut et au bas de l'écran.
5. Vous pouvez alors démarrer tous les logiciels de votre choix.

<< Retour

3. Sources documentaires

- Commentçamarche.net / Forum
- Grand dictionnaire terminologique
- Wikipedia (anglais)

<< Retour

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Restauration de système dans Windows

1. Les points de restauration

Le système d'exploitation Windows offre la fonctionnalité de restauration de système, qui permet à un utilisateur de ramener la configuration de Windows à un état antérieur si un problème survient. Pour y arriver, il doit utiliser les points de restauration.

Qu'est-ce qu'un point de restauration? Il s'agit d'un enregistrement, effectué à un moment donné, de tous les paramètres de Windows. Bref, c'est un peu comme si l'on prenait une photo de Windows à un moment précis. Si un problème survient, il est alors possible de revenir à l'état où Windows était au moment de la prise de photo.

IMPORTANT

Certains points de restaurations sont créés automatiquement (périodiquement, lors de l'installation d'un logiciel, etc.). Vous pouvez également créer vos propres points de restauration.

Une telle fonctionnalité est bien utile pour divers problèmes :

- Une mauvaise configuration qui compromet le fonctionnement du système d'exploitation;
- Un ou plusieurs logiciels malveillants qui ont été éradiqués, mais qui ont endommagé le système d'exploitation;
- L'installation d'un logiciel qui s'est mal déroulée ;
- Etc.

Dans de tels cas, il est souhaitable de restaurer la configuration de Windows. C'est possible de le faire en ramenant le système d'exploitation à un point de restauration antérieur où tout fonctionnait bien.

ATTENTION

Les points de restaurations ne servent qu'à restaurer des paramètres de Windows. Ils ne peuvent malheureusement pas restituer les autres logiciels ni les fichiers personnels (documents, photos, etc.).

<< Retour

2. La restauration de système sous Windows XP et Windows Vista

1. Cliquez sur le bouton « Démarrer » dans le coin inférieur gauche de votre écran;
2. Glissez votre curseur sur « Tous les programmes », puis sur « Accessoires »;
3. Glissez ensuite votre curseur sur « Outils système », puis sur « Restauration du système »;
4. L'interface des points de restauration apparaîtra. Vous pourrez y créer un point de restauration ou encore, revenir à un point de restauration antérieur.

<< Retour

3. La restauration de système sous Windows 7

1. Cliquez sur le bouton « Démarrer » dans le coin inférieur gauche de votre écran;
2. Dans la zone de recherche, tapez « Restauration du système »;
3. Dans la liste des résultats, choisissez « Restauration du système »;
4. L'interface des points de restauration apparaîtra. Vous pourrez y créer un point de restauration ou encore, revenir à un point de restauration antérieur.

<< Retour

4. Sources documentaires

- Aide et support de Microsoft
- Commentçamarche.net / Forum
- Wikipédia (français)

<< Retour

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

LIENS

À la recherche de ressources documentaires ou de gratuiciels à télécharger?

Cette section met à votre disposition une série d'hyperliens vers des sites pertinents pour vos différentes recherches d'information, et une liste de logiciels gratuits à télécharger pour renforcer votre sécurité.

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet
Maîtrise en études françaises, cheminement communication et langages
Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

Ressources

Sources d'information

- Assiste.com
- Secuser.com
- Commentçamarche.net
- Institut de la sécurité de l'information du Québec (ISIQ)
- Je protège mon identité sur Internet
- L'indispensable pour Internet, de Sébastien Sauvage

Sites d'actualités

- Technaute
- Silicon.fr
- Synchro-Blogue
- Branchez-vous Techno

Sites de téléchargement

- Free Downloads Center (anglais)
- Commentçamarche.net / Télécharger
- Download.com (anglais)

Forums

- Commentçamarche.net / Forum
- Clubic
- Vulgarisation informatique / Forum
- Yahoo! Québec : Questions - Réponses

Encyclopédies de logiciels malveillants et autres risques

- Symantec
- McAfee (anglais)
- Panda Security (anglais)

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour : 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement comunication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et securitaire

Télécharger

Pare-feu

- Outpost Firewall (anglais)
- Comodo Firewall (anglais)
- Matousec.com : résultats d'analyse (anglais)

Logiciels antivirus

- Avast
- Antivir
- AV-Comparatives.org : rapports annuels (anglais)

Logiciels antiespiogiciels

- Spybot Search & Destroy (anglais)
- Ad-Aware (anglais)
- Emisoft Anti-Malware (anglais)
- Windows Defender (avant de télécharger, vérifier si vous ne l'avez pas déjà sur votre ordinateur)

Logiciels de protection antiespiogicielle en temps réel

- SpywareBlaster (anglais)
- Windows Defender (avant de télécharger, vérifier si vous ne l'avez pas déjà sur votre ordinateur)

Logiciels antirootkit

- Sophos Anti-Rootkit (anglais)
- Rootkit Revealer (anglais)

Logiciels de courriel

- Mozilla Thunderbird
- Eudora (anglais)

Logiciels « de ménage »

- CCleaner
- Advanced SystemCare

Logiciel de désinstallation

- Revo Uninstaller

Logiciels de rechange

- **Messagerie instantanée :** aMSN (anglais), Pidgin (anglais) ou Trillian (anglais)
- **Lecture de PDF :** Foxit Reader (anglais)
- **Lecteur de musique :** Winamp ou Songbird (anglais)
- Et encore plus

Navigateurs

- Mozilla Firefox
- Opera
- Google Chrome

Autres

- Noscript (module complémentaire à Mozilla Firefox pour bloquer l'activation des sripts sur les sites Web)

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un memoire production sur la sécurité Internet

Maîtrise en etudes françaises, cheminement comunication et langages

Université de Sherbrooke. 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

SOURCES DOCUMENTAIRES

Sites Web

AGNITUM. *Outpost Firewall Free*, 2010, http://free.agnitum.com/.

ANTIPHISHING WORKING GROUP. *APWG*, 2010, http://www.antiphishing.org/.

AVAST SOFTWARE A.S. *Avast! Be free*, 2010, http://www.avast.com/fr-fr/index.

AVIRA. *Antivirus gratuit – Avira Antivir*, 2010, http://www.free-av.com/fr/index.html.

BEST SECURITY TIPS. *Best Security Tips*, 2010, http://www.bestsecuritytips.com/.

CLUBIC. *Clubic : Actualité informatique, Comparatifs, Logiciels et Forum*, 2010, http://www.clubic.com/.

COMMENTCAMARCHE.NET. *Forum d'assistance informatique*, 2010, http://www.commentcamarche.net/forum/.

CNET. *Download.com*, 2010, http://download.cnet.com/windows/.

DIRECTION INFORMATIQUE. *Direction informatique | technologies de l'information, TI, communications, stratégies*, 2010, http://www.directioninformatique.com/.

EQUIFAX INC. *Solutions personnelles. Dossiers de crédit, Scores de crédit, Protection contre le vol d'identité*, 2010, http://www.equifax.com/home/fr_ca.

FONDATION INTERNET NOUVELLE GÉNÉRATION (FING) et autres. *InternetActu.net*, 2010, http://www.internetactu.net/.

FREE DOWNLOADS CENTER. *Free Downloads Center - software and free game downloads*, 2009, http://www.freedownloadscenter.com/.

GENDARMERIE ROYALE DU CANADA (GRC) et autres. *PhoneBusters – Le centre d'appel antifraude du Canada*, 2010, http://www.phonebusters.com/francais/recognizeit_phishingemails.html.

GET SAFE ONLINE. *Get Safe Online*, 2010, http://www.getsafeonline.org/.

HOAXBUSTER.COM. *HoaxBuster - Premiere ressource francophone sur les hoax*, 2009, http://www.hoaxbuster.com/.

HOAXKILLER.FR. *Hoaxkiller.fr, moteur de recherche anti-hoax*, 2008, http://www.hoaxkiller.fr/.

INFORMACTION. *NoScript*, 2010, http://noscript.net/.

INSTITUT DE SÉCURITÉ DE L'INFORMATION DU QUÉBEC (ISIQ). *ISIQ*, 2009, http://www.isiq.ca.

INSTITUT DE SÉCURITÉ DE L'INFORMATION DU QUÉBEC (ISIQ). *Je protège mon identité sur Internet*, 2009, http://monidentite.isiq.ca.

INTERNET SYSTEMS CONSORTIUM. *Internet Systems Consortium*, 2010, https://www.isc.org/.

INTERNET WORLD STATS. *World Internet Usage Statistics News and World Population Stats*, 2010, http://www.internetworldstats.com/stats.htm.

JUD, Emmanuel. *Secuser.com – Sécurité informatique et protection de la vie privée*, 2010, http://www.secuser.com/index.htm.

KAMINSKY, Dan. *DoxPara Research*, 2008, http://www.doxpara.com/.

KASPERSKY LAB. *Viruslist.com - Information Sur les Virus, les Hackers et les Spams*, 2010, http://www.viruslist.com/fr/index.html.

LAVASOFT. *Ad-Aware by Lavasoft - Antivirus software, free spyware removal, firewall*, 2010, http://www.lavasoft.com/?domain=lavasoftusa.com.

LE JARGON FRANÇAIS. *Jargonf:Accueil – Le Jargon Français 4.1 – dictionnaire d'informatique*, 2010, http://jargonf.org/wiki/Accueil.

MALWAREBYTES. *Malwarebytes Blog*, 2010, http://malwarebytes.besttechie.net/ (Site temporairement hors ligne).

MCAFEE. *McAfee - Antivirus Software and Intrusion Prevention Solutions*, 2010, http://www.mcafee.com/ca-fr/?langid=48.

MEMOCLIC. *MemoClic, cliquez utile!*, 2010, http://www.memoclic.com/.

MSN.FR. *Dicos – MSN Encarta*, 2009, http://fr.encarta.msn.com/encnet/features/dictionary/dictionaryhome.aspx.

NARAYAN, *Bharath M. Bharath's Security Blog*, 2010, http://bharath-m-narayan.blogspot.com/.

NET MARKET SHARE. *Market share for browsers, operating systems and search engines*, 2010,

http://marketshare.hitslink.com/.

NETMEDIA EUROPE FRANCE. *Silicon.fr*, 2010, http://www.silicon.fr/.

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. *Grand dictionnaire terminologique*, 2010, http://www.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp.

PCWORLD COMMUNICATIONS INC. *Reviews and News on Tech Products, Software and Downloads – PCWorld*, 2010, http://www.pcworld.com/.

PINARD, Pierre. *Assiste.com – Sécurité informatique et protection de la Vie privée sur l'Internet*, 2008, http://assiste.com.free.fr/index.html.

REASONABLE SOFTWARE HOUSE LIMITED. *Reasonable Anti-phishing*, 2007, http://antiphishing.reasonables.com/PhishTest.aspx?Case=2.

SAFER NETWORKING LTD. *Spybot Search&Destroy*, 2010, http://www.safer-networking.org/fr/download/index.html.

SOFTPEDIA. *Free Downloads Encyclopedia – Softpedia*, 2010, http://www.softpedia.com/.

SYMANTEC. *Solutions antivirus, de sécurité et de disponibilité : Symantec Corporation*, 2010, http://www.symantec.com/fr/ca/index.jsp.

SYMPATICO.CA. *Synchro Blogue*, 2010, http://www.synchro-blogue.com/.

TRANSUNION. *TransUnion Canada*, 2010, http://www.transunion.ca/ca/home_fr.page.

UBM TECHWEB. *Security News brought to you by TechWeb*, 2010, http://www.techweb.com/security.

WHO.IS. *Who.is: Whois, Website, Domain Name, and IP Tools*, 2010, http://www.who.is/.

WIKIPEDIA. *Wikipedia, the free encyclopedia*, 2010, http://en.wikipedia.org/wiki/Main_Page.

WIKIPÉDIA. *Wikipédia, l'encyclopédie libre*, 2010, http://fr.wikipedia.org/wiki/Accueil.

Extraits de site Web

AV-COMPARATIVES. « Summary Reports », *AV-Comparatives*, 2010, http://www.av-comparatives.org/comparativesreviews/main-tests/summary-reports .

CNET NETWORKS. « Cookie », *Internet Security Zone.com*, 2010, http://fr.internetsecurityzone.com/Glossary/Cookie.

CNET NETWORKS. « Logiciel espion », *Internet Security Zone.com*, 2010, http://fr.internetsecurityzone.com/Glossary/Spyware.

CNET NETWORKS. « Logiciel publicitaire », *Internet Security Zone.com*, 2010, http://fr.internetsecurityzone.com/Glossary/Adware.

EMSI SOFTWARES. « Emisoft Anti-Malware », *Emisoft*, 2010, http://www.emsisoft.fr/fr/software/antimalware/.

ESET. « Scanner en ligne ESET – ESET NOD32 Antivirus 4 », *ESET*, 2010, http://www.eset-nod32.fr/scanner.html.

FACEBOOK. « Salle de presse, Statistiques », *Facebook*, 2010, http://www.facebook.com/press/info.php?statistics.

FILEHIPPO. « Download Piriform CCleaner », *Filehippo*, 2010, http://www.filehippo.com/download_ccleaner/.

FUTURA-SCIENCES. « Rootkit », *Futura-Techno*, 2010, http://www.futura-sciences.com/fr/definition/t/internet-2/d/rootkit_4030/.

IOBIT. « Advanced SystemCare Free Download », *Iobit*, 2010, http://www.iobit.com/advancedwindowscareper.html?Str=download.

JAVACOOL SOFTWARES. « SpywareBlaster », *Javacool Softwares*, 2010, http://www.javacoolsoftware.com/spywareblaster.html.

MALEKAL. « Gestion des utilisateurs sous Windows », *Malekal, forum d'aide informatique*, 2010, http://www.malekal.com//gestion_utilisateur_windows.php.

MATOUSEC. « Proactive Security Challenge: Results and comments », *Matousec.com*, 2010, http://www.matousec.com/projects/proactive-security-challenge/results.php.

MICROSOFT CORPORATION. « Aide et support Microsoft », *Microsoft*, 16 septembre 2010, http://support.microsoft.com/?LN=fr-ca&x=17&y=12.

MICROSOFT CORPORATION. « Microsoft Online Privacy Statement », *Microsoft*, 2010, http://privacy.microsoft.com/fr-ca/fullnotice.mspx.

MICROSOFT CORPORATION. « Principaux éléments de la Déclaration de confidentialité de Microsoft Online », *Microsoft*, 2010, http://privacy.microsoft.com/fr-ca/default.mspx.

MICROSOFT CORPORATION. « Watch out for fake virus alerts », *Microsoft Security*, 2010, http://www.microsoft.com/security/antivirus/rogue.aspx.

MICROSOFT CORPORATION. « Windows® Defender », *Microsoft Centre de téléchargement*, 2010, http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=435BFCE7-DA2B-4A6A-AFA4-F7F14E605A0D.

PANDA SECURITY. « Virus, Worms, antivirus and Security Information. », *Panda Security*, 2010, http://www.pandasecurity.com/homeusers/security-info/?sitepanda=particulares.

SOPHOS. « Sophos Anti-Rootkit », *Sophos*, 2010, http://www.sophos.fr/products/free-tools/sophos-anti-rootkit.html.

TREND MICRO. « Trend Micro HouseCall », *Trend Micro*, 2010, http://housecall.trendmicro.com/fr/.

VS REVO GROUP. « Revo Uninstaller Download », *VS Revo Group*, 2010, http://www.revouninstaller.com/revo_uninstaller_free_download.html.

VULGARISATION-INFORMATIQUE. « Forum informatique », *Vulgarisation informatique.com*, 2010, http://www.vulgarisation-informatique.com/forum-informatique.php.

YAHOO! QUÉBEC. « Questions et réponses, Informatique et Internet », *Yahoo! Québec*, 2010, http://qc.answers.yahoo.com/dir/index?link=list&sid=396545660.

ZDNET. « Phishing vs. Pharming », *ZDNET*, 2005, http://www.zdnet.com/videos/whiteboard/phishing-vs-pharming/153441.

Extrait d'émission de télévision

CAROLL, Jason. « Internet cell phone popcorn HOAX - secret revealed », *CNN* [par YouTube], [s. d.], http://www.youtube.com/watch?v=KsoVEeJg3TY.

Articles de périodiques Internet

CAUCHON, Paul. « Mafiaboy, l'ado qui a fait tomber Yahoo!, eBay et CNN », *Le Devoir*, 1er novembre 2008, http://www.ledevoir.com/culture/livres/213623/mafiaboy-l-ado-qui-a-fait-tomber-yahoo-ebay-et-cnn.

CONDO, Jean-Charles. « Loi anti-pourriel Can-Spam : conclusion d'une première affaire », *Branchez-vous! Techno*, 12 octobre 2004, http://www.branchez-vous.com/actu/04-10/08-313901.html.

CONDO, Jean-Charles. « Mac OS X: un cheval de Troie déguisé en vidéo osée de Leighton Meester », *Branchez-vous! Techno*, 25 juin 2009, http://techno.branchez-vous.com/actualite/2009/06/mac_osx_un_cheval_de_troie_deg.html.

COGSWELL, Bryce et Mark RUSSIINOVICH. « RootkitRevealer v1.71 », *Windows Sysinternals, Microsoft TechNet*, 1er novembre 2006, http://technet.microsoft.com/fr-fr/sysinternals/bb897445%28en-us%29.aspx.

DUMAIS, Nelson. « Sachant que le pire est à venir... », *La chronique de Nelson*, 25 novembre 2008, http://blogues.cyberpresse.ca/technaute/dumais/2008/11/25/sachant-que-le-pire-est-a-venir/.

GRONDIN, Alexis. « Les réseaux sociaux sont de vrais annuaires pour les cybercriminels », *01Net Pro*, 24 juillet 2008, http://pro.01net.com/editorial/387450/les-reseaux-sociaux-sont-de-vrais-annuaires-pour-les-cybercriminels/.

JOHNSON, Maxime. « Conficker infecte 50 000 nouveaux PC par jour », *Branchez-vous! Techno*, 21 mai 2009, http://techno.branchez-vous.com/actualite/2009/05/conficker_infecte_50_000_nouve.html.

LEDUC, Christian. « Conficker se déploie progressivement », *Branchez-vous! Techno*, 27 avril 2009, http://techno.branchez-vous.com/actualite/2009/04/conficker_se_deploie_progressi.html.

RADIO-CANADA, AGENCE FRANCE-PRESSE, PRESSE CANADIENNE et BBC. « Une importante brèche colmatée », *Radio-Canada*, 10 juillet 2008, http://www.radio-canada.ca/nouvelles/societe/2008/07/09/001-faille-informatique.shtml.

TECHNAUTE. « Mafiaboy raconte son histoire », *Technaute*, 8 octobre 2008, http://technaute.cyberpresse.ca/nouvelles/internet/200810/06/01-26824-mafiaboy-raconte-son-histoire.php.

ITESPRESSO.FR. « Le roi du spam condamné à 47 mois de prison aux États-Unis », *ITEspresso.fr*, Traduction de l'article « Spam King Soloway sent down for 47 months » de *VUNet*, 24 juillet 2008, http://www.itespresso.fr/le-roi-du-spam-condamne-a-47-mois-de-prison-aux-etats-unis-22426.html.

WEBMASTER HUB. « Pharming : encore plus dangereux que le phishing! », *WebMaster Hub*, 18 octobre 2006, http://www.webmaster-hub.com/publication/Pharming-encore-plus-dangereux-que.html.

Documents Web en format PDF

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE). *Orientations de l'OCDE pour les politiques sur le vol d'identité en ligne*, 2008, http://www.oecd.org/dataoecd/51/59/40883671.pdf, 23 p.

Livres

BEAVER, Kevin. *Combattre les Hackers pour les nuls*, Coll. « Pour les nuls », Traduction de B. Jolivart et P. Escartin, Paris, Éditions First Interactive, 2004, 423 p.

CHARTON, ÉRIC. *Spywares et virus : Protégez-vous des logiciels escrocs*, Coll. « Kit Campus », Paris, CampusPress, 2005, 245 p.

GOMEZ URBINA, Alexandre. *Hacking interdit*, 2e édition, Coll. « microapp », Paris, Micro Application, 2007, 1247 p.

GRALLA, Preston. *PC Pest Control*, Sebastopol, O'Reilly Media Inc., 2005, 275 p.

KONG, Joseph. *Rootkits BSD : Mieux les comprendre pour mieux s'en protéger*, Paris, Campus Press, 2007, 148 p.

LEVINE, John R. *Sécurité Internet pour les nuls*, Paris, Éditions First Interactive, 2003, 398 p.

MITNICK, Kevin David. *L'art de la supercherie : les révélations du plus célèbre hacker de la planète*, Paris, CampusPress, 2005, 377 p.

SCHILLER, Craig A. et Jim BINKLEY, David HARLEY, Gadi EVRON, Tony BRADLEY, Carsten WILLEMS, Michael CROSS. *Botnets : The Killer Web App*, [s.l.], Syngress Publishing, Inc., 2007, 464 p.

TRABELSI, Zouheir et Henri LY. *La sécurité sur Internet*, Paris, Hermès Science Publications, 2005, 254 p.

Articles de périodiques

AZZEMOU, Sam. « La sécurité de votre PC : ce qui marche vraiment en 32 questions », *Micro Actuel*, no 46, p. 38 – 46.

DUVAL, Loïc. « 12 suites de sécurité au banc d'essai », *Micro hebdo*, no 608, 10 décembre au 16 décembre 2009, p. 20 – 27.

GRANGER, Jérôme, RODA, José et Jérôme SAIZ. « Halte aux nouveaux dangers du Web », *L'ordinateur individuel*, no 203, mars 2008, p. 64 – 79.

PICARD, François. « Des précautions à prendre pour se protéger en ligne », *Atout Micro*, Vol. 21, no 7, avril 2008, p. 12 – 15.

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises, cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

PLAN DU SITE

- **Accueil**
  - Un peu d'histoire
  - Objectif du site
- **Glossaire**
  - A - C
  - D - L
  - M - P
  - Q - Z
  - Sources documentaires
- **Menaces**
  - Logiciels malveillants
    - Cheval de Troie (*Trojan Horse*)
    - Espiogiciel (*Spyware*)
    - Faux logiciel de sécurité (*Rogue security software*)
    - Logiciel publicitaire (*Adware*)
    - Trousse administrateur pirate (*Rootkit*)
    - Ver informatique (*Worm*)
    - Virus
  - Autres fraudes et trompreries
    - Canular (*Hoax*)
    - Hameçonnage (*Phishing*)
    - *Pharming*
    - Pourriel (*Spam*)
    - Témoin traceur (*Tracking Cookie*)
- **Aide au diagnostic**
  - Questions + Réponses
    - C'est la panique!
    - Je suis inquiet... ou exaspéré
    - Je veux me renseigner
  - Liste de bonnes habitudes et attitudes à emporter
- **Faits divers**
  - Vie privée
    - Bien choisir son mot de passe

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises cheminement communication et langages

Université de Sherbrooke, 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

CONDITIONS D'UTILISATION

1. **Droits d'auteur**
   i. Le présent site Web est le résultat de recherches effectuées dans le cadre d'une maîtrise en études françaises, cheminement communication et langages, complétée à l'Université de Sherbrooke (Québec).
   ii. L'ensemble des contenus du présent site Web (« le site »), incluant textes et images, sont la propriété exclusive d'Annie Varin (« l'auteure »).
   iii. Reproduction du contenu
      a. Toute reproduction privée et (ou) commerciale est strictement interdite, sauf sous l'approbation écrite de l'auteure. Les demandes de reproduction peuvent être formulées à partir de la page suivante : Contact.
      b. Toute reproduction non privée et (ou) non commerciale peut être effectuée sans demande d'autorisation de l'auteure. Toutefois, l'utilisateur se doit de :
         - identifier clairement le nom du site et son adresse URL en tant que source de la reproduction;
         - s'assurer de l'exactitude de la reproduction;
         - aviser l'auteure de la reproduction à partir de la page suivante : Contact.

2. **Contenu du site**
   i. Ce site propose de l'information pour prévenir et idéalement guérir les problèmes technologiques liés à l'utilisation d'Internet, ce qui inclut la protection des données confidentielles des internautes, et il se concentre sur cet objet avec exclusivité. Les problèmes de nature « sociale » occasionnés, en tout ou en partie, par Internet (pédophilie, violence, pornographie, etc.) ne font pas partie des sujets traités.
   ii. Toute mention d'ordre technologique dans ce site fait référence à la plateforme Windows en raison de la forte majorité internaute employant ce système d'exploitation.
   iii. Sauf en cas d'avis contraire, les procédures sont valides pour les systèmes d'exploitation

Windows XP, Windows Vista et Windows 7.

iv. Les propos tenus reflètent l'opinion de l'auteure et doivent être perçus à titre de suggestions. L'utilisateur n'est pas dans l'obligation de les respecter.

v. Rectification

a. Si l'utilisateur constate une erreur dans le contenu, il peut faire une demande de rectification. Toute demande de rectification de contenu peut être formulée à partir de la page suivante : Contact. Pour être conforme, elle doit être fondée et contenir (« les critères de rectification ») :

- L'hyperlien de la page où se trouve le contenu;
- La rectification proposée en soi;
- Au moins une (1) source crédible pour l'appuyer. La crédibilité de ladite source est à la discrétion de l'auteure.

b. La rectification sera analysée par l'auteure, qui en vérifiera l'exactitude et qui décidera ensuite si une correction doit être apportée. Toute demande non fondée et (ou) ne respectant pas les critères de rectification sera automatiquement refusée.

3. **Hyperliens**

i. Le site contient plusieurs hyperliens menant vers des sites Web externes (de couleur vert-turquoise). L'auteure a choisi les hyperliens avec grand soin, mais n'est pas responsable de la fiabilité de l'information fournie sur ces sites externes.

ii. Chaque hyperlien externe menant vers un site anglophone comporte une mention « anglais ».

a. Logiciels à télécharger : la mention « anglais » ne concerne que le site Web où le téléchargement peut être effectué. Il est possible que le logiciel en question soit disponible en français, même si le site où il peut être téléchargé n'est offert qu'en anglais.

iii. Les efforts nécessaires seront mis en œuvre pour mettre méticuleusement à jour tout lien vers un site externe s'avérant désuet, inexact et (ou) non pertinent.

4. **Confidentialité**

i. Tout utilisateur peut circuler librement dans le site sans être dans l'obligation de révéler son identité ou de fournir des renseignements personnels.

a. Sur la page « Liste de bonnes habitudes et attitudes... à emporter », l'utilisateur est invité à révéler son prénom dans le seul but de personnaliser la liste générée avec cette page. Cette donnée ne sera pas enregistrée.

b. Sur la page « Contact », l'utilisateur est invité à inscrire son adresse courriel afin de permettre à l'auteure d'établir une communication par la suite, si nécessaire. Cette donnée ne sera pas enregistrée.

ii. Aucun témoin (*cookie*) ne sera installé sur l'ordinateur de l'utilisateur au cours de la visite.

Note : Le genre masculin a été utilisé dans le seul but d'alléger le texte.

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet

Maîtrise en études françaises cheminement communication et langages

Université de Sherbrooke 2011

SÉCURITÉ INTERNET 101
Technologie et comportement

Utiliser Internet de manière intelligente et sécuritaire

CONTACT

Adresse courriel :

Sujet :
Choisissez...

Contenu du message :

Question de sécurité :
(pour m'assurer que vous êtes bien une personne et non pas un bot informatique malicieux;-)

Combien y a-t-il d'heures dans une journée?

Envoyer Recommencer

Accueil | Glossaire | Menaces | Aide au diagnostic | Faits divers | Liens

Sources documentaires | Plan du site | Conditions d'utilisation

Dernière mise à jour 4 janvier 2011

Ce site a été conçu dans le cadre d'un mémoire production sur la sécurité Internet
Maîtrise en études françaises cheminement communication et langages
Université de Sherbrooke 2011