Sécurité INTERNET

- Débutant intéressé - INTERNET -

Date de mise en ligne : samedi 10 mai 2008

Aides en Informatique

On ne m'a pas dit ce que c'est réellement la sécurité sur INTERNET.

Je souhaite payer en ligne mes impôts ou faire mes achats sur le WEB.

Introduction

INTERNET est un réseau d'informations dont il faut savoir se servir. Se servir d'INTERNET correctement consiste à être journaliste. Nous allons présenter une approche afin d'utiliser ce réseau.

Toute réalisation humaine est créée afin d'arriver à des objectifs donnés, que ce soit dans le gratuit ou dans le payant. On peut deviner ces objectifs en lisant les règles internes des Sites Web. Il y aussi les philosophies des administrateurs de l'autorité, entreprise ou association.

L'insécurité quelle qu'elle soit se résout par la compréhension des systèmes de confiances humains.

L'adresse INTERNET

L'adresse INTERNET avec le protocole http indique que vous êtes sur le réseau INTERNET non sécurisé source d'information. L'adresse complète d'accès à l'accueil du site identifie le Site Web. Reste à vérifier s'il est sur ses sites Web de confiance autres que les moteurs de recherche.

L'adresse INTERNET sécurisée avec le https indique que vous êtes en train de faire une transaction sécurisée voire de fournir des informations à cette source d'information. Si le site web n'a pas payé une autorité de confiance vous avez un message vous demandant d'approuver votre confiance ci-après.

Le protocole https affiche une page d'alerte si le site web n'est pas certifié

Sachez que le protocole https ne signifie pas que le site web est de confiance, même si vous ne voyez pas cette page. Il faut vérifier si le site web est de confiance à partir d'autres sites web de confiance.

Le chapitre précédent vous montre ce qu'est un nom de domaine, connaissance prépondérante pour connaître une source de confiance.

Les certificats

Les certificats qui existent dans le protocole https permettent de certifier un site web. On peut les rencontrer sur son navigateur.

Ce sont des systèmes de sécurité qui contiennent une information d'autorisation et peuvent modifier des données sur l'ordinateur, tout comme le protocole http. Sur LINUX ils ne peuvent pas modifier l'environnement si vous n'avez pas tapé votre mot de passe administrateur avant de démarrer votre navigateur web.

Il faut vérifier cette information d'autorisation et vérifier si l'autorité qui l'a délivrée est un site de confiance. Le certificat peut avoir expiré auquel cas il n'est plus crédible.

Le paiement

Un paiement sécurisé doit s'effectuer selon les protocoles de sécurité applicables au pays. Toute connexion sécurisée entièrement enregistrée est cassable.

Internet est un réseau maillé. c'est à dire qu'il relie les villes par plusieurs chemins. Une île possède peu de mailles.

Le paiement doit donc se faire dans le réseau INTERNET continental afin que les informations ne passent pas par la même maille. Il est donc impossible d'acheter facilement en Angleterre avec une carte bancaire à partir de la France, mis à part via un serveur français PAYPAL situé en dehors de l'Angleterre. En effet l'Angleterre est une île et dispose donc de peu de mailles.

Bien-sûr un paiement fait dans un pays instable se fait à vos propres risques. Encore faut-il savoir quel pays est instable.

Le paiement par INTERNET doit suivre les évolutions techniques et humaines de son pays. On peut demander à sa banque une carte bancaire plus sécurisée. Ce service est payant il faut donc avec faire beaucoup d'achats sur INTERNET sans qu'il y aie une partie supplémentaire à payer.

De même un paiement dans un pays en plein essor donne plus de chances de se faire délivrer un article.

Attention !

"les règles de paiement et de Service Après Vente changent en fonction des pays."

Les Sites de Commerce Électronique

Il est facile de trouver des sites de commerce électronique de confiance. Il suffit pour cela de vérifier s'ils sont sur des sites autres que les moteurs de recherche de commerce électronique comme par exemple des sites de consommateurs.

Seul un article réceptionné indique que l'on a à faire à un site de vente. Si le site est lié à un site de consommateurs c'est que le site de commerce possède des consommateurs. Encore faut-il que ces consommateurs aient un avis objectif.

Les sites de commerce électroniques qui ne respectent pas les autorités de leur pays sont dits hors-la-loi. Il faut donc vérifier s'ils respectent les lois de leur pays avant d'acheter. C'est ce que font les moteurs de recherche de commerce électronique. Seulement ils ne vont vérifier que ce qui doit être respecté. Donc ils vont aider à ce que les autres sites de commerce respectent la loi.

Les courriels ou messages non désirés

Si des messages non désirés arrivent dans votre messagerie électronique il est possible d'utiliser THUNDERBIRD ou EVOLUTION qui possèdent un anti-publicité automatique (cf chapitre Messagerie Anti-Spam).

Les médias

Avant de lire un média il faut connaître sa ligne éditoriale. Si elle n'est pas connue ou non respectée cela demande à ce que le lecteur s'interroge. Les lignes éditoriales se trouvent sur le Site Web dans la présentation du média ou bien lorsque leurs journalistes montrent leurs convictions. Il s'avère qu'un journaliste doit suivre la ligne éditoriale de son journal. Donc cela indique ce que l'on va la retrouver sur le média. La ligne éditoriale doit être consultable.

On peut retrouver la ligne éditoriale d'un média en analysant les textes les plus récurrents. On peut analyser les mots utilisés ou l'orientation des articles en fonction des thèmes. L'orientation des articles doit normalement être différente en fonction du journaliste. Sinon cela veut dire que la ligne éditoriale du Média est trop limitée donc que le média n'est pas crédible.

Les médias qui font participer les lecteurs en direct peuvent être crédibles. Encore faut-il que l'on ne retrouve pas des stéréotypes ou pire des clichés. Il faut que le lecteur postant des messages soit objectif lui aussi. Si votre message envoyé sur le site web est immédiatement affiché il y a de grandes chances que les avis soient objectifs. Sinon cela veut dire que le média n'informe pas. Les sites participatifs n'ont pas de ligne éditoriale et ont des lecteurs s'exprimant librement donc ils sont crédibles.

Il faut faire attention à la répétition des phrases de même nature et se méfier de cette redondance. Si on avale la redondance cela veut dire que l'on manque soit même d'objectivité. Une information illogique n'a pas besoin d'être prouvée puisque le manque de logique indique un déni de sens donc une désinformation.

Il faut avoir l'avis de chaque camp avec les personnes qui les représentent. Attention à bien retenir qu'un camp qui se méfie des médias cherche à trouver de la crédibilité ou de la légitimité. Si l'avis de chaque camp devient un stéréotype c'est que les informations n'évoluent pas donc que le média n'est pas crédible. Cela ne veut dire en aucun cas que le camp n'est pas crédible si l'avis du camp ne se donne pas en direct.

Un vocabulaire familier utilisé par un média montre son manque d'objectivité. On n'apprécie guère le vocabulaire familier lorsqu'on écoute ou pire lorsqu'on lit un média. Cela a en effet pour objectif de dévaloriser le camp représenté.

Problème de piratage informatique

On peut facilement penser qu'on est sur une liste noire avec un ordinateur. Il est à savoir que lorsque quelqu'un veut vraiment du mal on peut difficilement travailler sur l'ordinateur. Puis rapidement on ne peut plus rien faire. Les données importantes qui relèvent de la sécurité personnelle sont liées à l'appât du gain. Il faut donc supprimer toute information liée à l'argent d'un réseau public voire de son ordinateur personnel.

Sinon on a souvent à faire à un ordinateur qui a notre adresse mail ou notre adresse d'ordinateur. Ce sont rarement les deux informations à la fois mais on a tendance à le penser du fait de l'identification facile sur le web. Il faut avoir été menacé pour penser que quelqu'un essaie de savoir quelque chose sur soi.

Si son ordinateur est spamé c'est peut-être un ver ou un troyen. Le ver et le troyen utilisent le réseau de votre ordinateur. Ils peuvent regarder dans l'ordinateur. Les informaticiens qui utilisent ces programmes s'intéressent à

l'argent donc il ne faut aucun numéro de carte bancaire sur votre ordinateur.

Le ver et le troyens ralentissent l'ordinateur. Il faut donc un anti-virus (CLAMTK ou AVAST) et un anti-spyware (WINDOWS uniquement car non protégé). Un système UNIX comme LINUX annihile l'action de ces programmes par les mises à jour donc un anti-virus peut être fortuit. Un troyen ne fait que regarder l'ordinateur donc il faut plutôt un pare-feu correctement installé sur ou derrière son modem.

Configurer un pare-feu

Un pare-feu est un appareil ou un logiciel de sécurité informatique. Il contient comme pour les navires des ports autorisants l'envoi ou la réception d'informations.

Pour configurer un pare-feu qui peut exister sur une box ou un routeur il faut en général verrouiller les ports UDP. Si on est plus paranoïaque on peut verrouiller tous les ports TCP et UDP sauf les ports TCP 80 et 21. Le port TCP 80 c'est le navigateur Web. Le 21 ce sont les téléchargements.

On dispose alors de moins de services INTERNET. Autorisez d'autres ports pour d'autres services de communication comme un téléphone ou un compte mail qui permet de tchater. Cherchez sur INTERNET « ports pare-feu nom_de_lapplication » puis activez ces ports.

Si on installe un pare-feu logiciel on peut en plus empêcher à certaines applications de communiquer sur INTERNET pour éviter d'être vu ou bien empêcher des troyens ou vers de communiquer. Dans ce cas il faut bien comprendre comment son ordinateur communique.
Un pare-feu contient en général l'historique des connexions extérieures appelé « log ». Il peut vous avertir d'attaques extérieures ou annihiler tout troyen en étant bien configuré. Ensuite LINUX vous aide à tracer les adresses IP dans les outils réseaux.