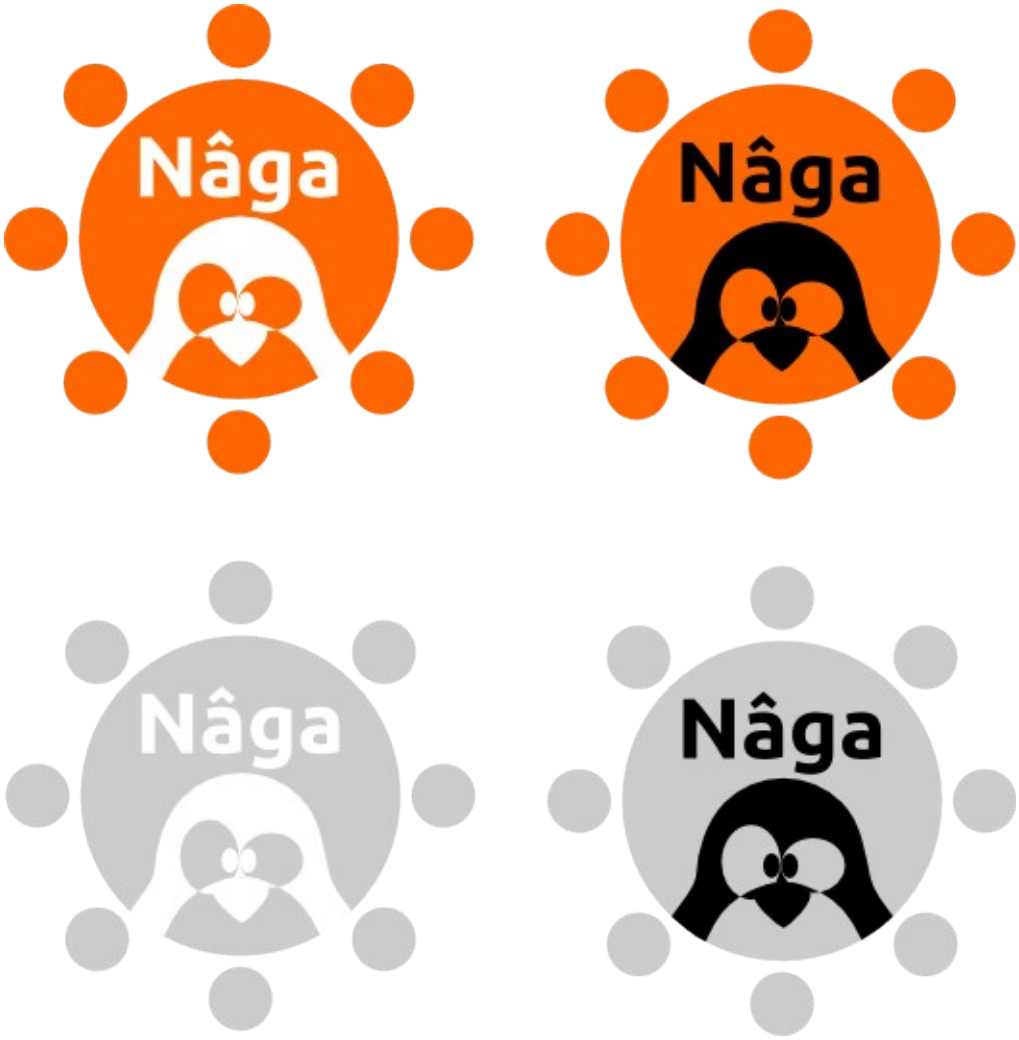
Formation « sécurité informatique »

Sous GNU/Linux



Le 27 février 2015

Droits d'auteurs

Sommaire

L'association Nâga

Qu'est ce que c'est ?

Le projet Nâga est une association loi 1901 basée sur Nantes Métropole, portant sur la prévention et la revalorisation des déchets informatiques, s'inscrivant ainsi dans une démarche propre au développement durable (solidarité, autonomie, diminution de l'impact carbone...).

Le siège social est situé à la Bonneterie, 17 chemin Fontaine Launay, 44 400 REZÉ.

Nous contacter

Par téléphone : 02 85 52 31 22

Courriel : contact@naga44.org

À travers le site : www.naga44.org

Quelles sont les activités ?

L'activité est concentrée sur la récupération d'ordinateurs, leur reconditionnement sous Linux et le don aux adhérents.

Le tarif de l'adhésion change en fonction des revenus :

Personnes allocataires de minimas sociaux (RSA, ASS, AAH...) : 40 euros

Personnes ayant des revenus compris entre les minimas et le SMIC inclus : 80 euros

Personnes ayant des revenus supérieurs au SMIC / associations : 120 euros

En parallèle des ateliers sur l'utilisation de logiciels seront proposés tout au long de l'année.

De plus, l'association assure des prestations sous forme de formations et de conceptions de sites internet.

Où sont les activités ?

Nos activités se dérouleront à la Bonneterie (17 chemin Fontaine LAUNAY, 44 400 Rezé).

Sécurité informatique

Présentation

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques et d'information. Enjeu majeur pour les entreprises depuis les débuts de l'Internet, elle reste cependant obscure et méconnue pour la plupart des utilisateurs ordinaires de l'informatique actuelle, ces derniers manquant cruellement d'informations essentielles et de sensibilisation sur le sujet, au grand détriment de leur vie privée et de leur liberté d'expression.

À l'heure où les fournisseurs d'accès à Internet ont les moyens, les raisons et la possibilité d'examiner presque toutes les communications entrantes et sortantes de votre ordinateur lorsque celui-ci est connecté, où les mastodontes de l'hébergement en ligne scannent sans complexes vos communications et contenus (e-mails, web et fichiers) à des fins marketing ou pire encore, où les contenus sensibles ou choquants sont accessibles aux plus jeunes sans réelles restrictions ni prévention, où des personnes malintentionnés s'attaquent à votre compte bancaire ou votre vie privée, il devient indispensable et judicieux de se protéger en sécurisant ses communications.

Pour exemple, voyez plutôt ci-dessous un extrait des conditions générales d'utilisation des services de *Google*, sur la version américaine de son site :

« *Nos systèmes automatisés analysent votre contenu (y compris les e-mails) pour vous diffuser des fonctionnalités pertinentes pour vous, comme des résultats de recherche personnalisés, de la publicité sur mesure, ... Cette analyse a lieu à la réception, à l'envoi et lors du stockage du contenu.* »

Attention, même si une partie des sujets traités ci-après concernent tous les systèmes d'exploitation, la présente formation est orientée vers la sécurité informatique sous les systèmes libres GNU/Linux. En effet, opter pour l'utilisation de ces derniers permet d'emblée de disposer d'une sécurité robuste contre les intrusions et les logiciels malveillants (virus, vers et chevaux de Troie), mais aussi d'avoir accès gratuitement à de nombreux outils logiciels libres d'analyse et de protection.

Lorsque vous souscrivez un abonnement d'accès à l'Internet, les informations concernant la sécurité manquent cruellement. Les fournisseurs d'accès commerciaux ne joignent pas de manuel explicite vous permettant de sécuriser aisément votre box, de naviguer en toute sécurité ou encore de protéger vos enfants. Le présent support tend à palier ce manque.

Les services d'Internet

Avant de se lancer dans le vif du sujet de la sécurité informatique, il est indispensable de revenir brièvement aux fondements de l'Internet pour rappeler que ce dernier n'est pas uniquement ce qu'on appelle communément le web, mais bien une multitude de réseaux d'ordinateurs interconnectés les uns aux autres utilisant les services d'Internet et leurs différents protocoles :

- **Web**, **www** ou **World Wide Web** (**HTTP** ou **H**yper**T**ext **T**ransfert **P**rotocol) : service de consultation d'hyper-documents (pages web), c'est le service d'Internet le plus connu et le plus utilisé.

- **Courrier** ou **e-mail** (**POP**, **IMAP**, **SMTP**): service de messagerie électronique permettant de déposer un courrier dans la boîte aux lettres de son correspondant, qu'il soit ou non devant son ordinateur ; à sa prochaine connexion, ce dernier sera capable de consulter sa boîte aux lettres pour lire son courrier et d'y répondre si besoin.

- **Transfert de fichiers** (**FTP** ou **F**ile **T**ransfer **P**rotocol) : service d'échange de fichiers permettant, à partir d'un ordinateur courant (client), de déposer ou télécharger des fichiers sur un ordinateur distant (serveur) à travers le réseau.

- **Chat** (**IRC** ou **I**nternet **R**elay **C**hat) : service de messagerie instantanée permettant de dialoguer en temps réel et de manière interactive avec un ou plusieurs correspondants, au travers de salons de discussions génériques ou à thèmes.

- **Forums** ou **News** (**NNTP** ou **N**etwork **N**ews **T**ransfert **P**rotocol) : service de messagerie en temps différé permettant à chaque utilisateur de déposer des messages, dans des rubriques à thèmes, afin de créer des sujets de discussions ou d'y participer.

GNU/Linux et logiciels malveillants

Avant tout, il est important de comprendre rapidement les différents types de logiciels malveillants (ou malware) auxquels on peut être confronté:

- *Le virus informatique* : programme exécuté à l'insu de l'utilisateur ayant la propriété de pouvoir créer des répliques de lui-même dans d'autres programmes (automate auto réplicatif). Il peut ensuite perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté (ralentissements, destruction de données, etc...), mais aussi se répandre par tout moyen d'échange de données numériques tels que les réseaux informatiques, CD/DVD, disques durs externes et clés USB, etc. Le virus de boot quand à lui ne modifie pas un programme comme le fait un virus normal, il a la particularité de s'installer dans un des secteurs de démarrage d'un disque dur ou d'une partition, pouvant ainsi modifier ou bloquer complètement le démarrage.

- *Le ver informatique* : programme exécuté à l'insu de l'utilisateur ayant la propriété de pouvoir se propager et de se dupliquer par ses propres moyens sans contaminer de programme hôte, en exploitant les différentes ressources de l'ordinateur qui l'héberge. Il peut se répandre par les mêmes moyens que les virus mais ses objectifs diffèrent sensiblement, et sont principalement l'espionnage de l'ordinateur infecté, son intrusion et/ou sa prise de contrôle, le vol et/ou la destruction de données ou encore l'envoi de multiples requêtes vers un serveur internet dans le but de le saturer (DDOS ou attaque par déni de service).

- *Le cheval de Troie* (ou *Trojan Horse*) : programme légitime en apparence contenant une malveillance et installé à l'insu de l'utilisateur. Il n'exécute aucune action en lui-même est sert uniquement de véhicule à l'installation d'un vrai parasite. Il peut contenir un virus, un ver ou tout autre logiciel espion.

- *Le logiciel espion* (*mouchard* ou *spyware*) : aujourd'hui très largement répandu sur internet, c'est un programme exécuté à l'insu de l'utilisateur, dans le but de collecter et récolter des informations sur l'utilisateur et/ou l'utilisation de l'ordinateur infecté. Plus gravement, il peut aussi tenir le rôle d'enregistreur de frappe (*keylogger*) et transmettre automatiquement tout ce qui est frappé sur le clavier à des fins de vol de mots de passe, de coordonnées bancaires et pire encore. Les principaux vecteurs d'infection sont très souvent des logiciels gratuits (*gratuiciel* ou *freeware*, *partagiciel* ou *shareware*), les *cracks* et *keygen*, les faux codecs, les barres d'outils, les faux logiciels/utilitaires de sécurité (*rogues*), les pièces jointes par e-mail et messagerie instantanée ou plus simplement en naviguant sur de très nombreux sites internet douteux, notamment ceux au contenu illégal ou pornographique.

Comme indiqué précédemment, les systèmes d'exploitation GNU/Linux permettent une protection accrue à plusieurs niveaux. Tout comme les autres systèmes, ils possèdent évidemment des failles de sécurité pouvant être exploitées par des programmes malveillants, mais dans une moindre mesure. Voyons pour quelles raisons :

- Par défaut, leurs utilisateurs n'ont pas les droits administrateur et ne peuvent donc pas modifier les fichiers système, ce qui rend la duplication et donc l'infection très difficile.
- L'obligation de préciser si un fichier est exécutable ou non rend une infection silencieuse laborieuse ; par exemple, impossible d'être infecté par fichier.jpg.exe en pensant que c'est un fichier image ; l'extension .exe étant destinée aux exécutables sous Microsoft Windows.
- Peu ou pas de services réseau ouverts, exemple sous ubuntu[1], la configuration par défaut du système est donc généralement plus sûre, la configuration avancée restant très robuste.
- Le code source étant ouvert, tout le monde peut l'examiner y compris les experts en sécurité, ce qui aide largement à une rapide détection et correction des failles de sécurité, contrairement aux systèmes d'exploitation propriétaires au code source fermé.
- Le téléchargement des logiciels libres dans des dépôt dont le contenu est contrôlé par la communauté permet d'éviter d'installer des logiciels infectés provenant de sites internet douteux ; ce principe rend l'utilisation d'antivirus radicalement et définitivement inutile.
- La grande quantité et variété des distributions GNU/Linux permettent de rendre la conception et la diffusion de logiciels malveillants beaucoup plus difficiles.
- Les développeurs de logiciels malveillants visent la plus grande part de marcher des ordinateurs de bureau, à savoir le système le plus utilisé, dans le but de toucher un maximum de victimes potentielles.

Auparavant, les serveurs d'entreprises restaient les cibles privilégiées d'attaques en tout genre mais depuis ces dix dernières années, le nombre croissant d'utilisateurs particuliers de GNU/Linux entraîne inévitablement une légère augmentation du développement de logiciels malveillants lui étant dédiés. Ainsi en 2005, la nombre de programmes malveillants pour GNU/Linux est passé de 422 à 863[2]; pas de panique cependant, la grande majorité des menaces sérieuses détectées restant des *rootkits*, conçus dans le but d'obtenir et pérenniser un accès non autorisé à un serveur et laissant de côté les ordinateurs de bureau des particuliers.

Notons au passage qu'à ce jour, hormis dans un but éducatif et de démonstration, il n'existe encore aucun cas concret d'infection virale d'espace utilisateur sous GNU/Linux. Pour preuve de sa fiabilité, sachez qu'en novembre 2013, GNU/Linux équipe au total 482 supercalculateurs des 500 les plus puissants au monde, soit une part de marcher de près de 96,4 %, suivi par UNIX sur 11 autres, 4 sur une combinaison de systèmes d'exploitation, 2 sous Windows et 1 sous BSD ![3]

1 http://guide.ubuntu-fr.org/desktop/net-firewall-on-off.html

2 http://www.internetnews.com/dev-news/article.php/3601946

3 http://www.developpez.com/actu/64718/Linux-equipe-plus-de-95-pourcent-du-top-500-des-supercalculateurs-les-plus-puissants-du-monde-Tianhe-2-garde-son-trone/

Sécuriser sa box Internet

Après avoir souscris une offre d'accès à internet chez un fournisseur, la première chose importante à faire lorsque vous avez reçu et connecté votre box (modem, routeur) est de la sécuriser convenablement, afin d'éviter qu'elle soit utilisée par une personne malintentionnée.

Le principe est sensiblement identique avec tous les FAI (fournisseur d'accès à Internet), vous devez avant tout accéder à l'interface de gestion de votre box, directement par le biais de la barre d'adresse de votre navigateur Internet (Firefox, Chromium, etc..) :

- pour la Livebox (Orange) : entrez le mot livebox puis pressez Entrer.
- pour la Bbox (Bouygues) : entrez 192.168.1.254 ou gestionbbox.lan puis pressez Entrer.
- pour la Freebox (Free) : entrez mafreebox.freebox.fr puis pressez Entrer.
- pour la Box de SFR : entrez 192.168.1.1 puis pressez Entrer.
- pour la Box d'OVH : entrez 192.168.1.254 puis pressez Entrer.

Nom du réseau wifi (SSID)

Ensuite, si vous souhaitez vous connecter à votre box en wifi, il est important de pouvoir la repérer facilement dans la liste des réseaux wifi disponibles aux alentours, pour cela il vous suffit de modifier son nom (SSID), dans la partie nommée Wifi de l'interface de gestion. Pour une sécurité accrue, vous pouvez également choisir de cacher ce nom afin que personne ne puisse détecter votre box et tenter de s'y connecter ; dans ce cas vous devrez le ré-afficher à chaque fois que vous voudrez paramétrer un de vos appareils pour qu'il puisse s'y connecter automatiquement.

Clé de sécurité wifi

Dans cette partie Wifi, vous trouverez également votre clé de sécurité (WEP ou WPA), qui vous sera nécessaire pour pouvoir vous connecter à votre box en wifi; en général si vous ne l'avez pas modifiée, vous pouvez la retrouver plus simplement au dos de votre box. Pour renforcer la sécurité d'accès, il est impératif d'utiliser une clé WPA, qui propose un chiffrement (cryptage) largement plus fiable, à ce jour inviolé si l'on désactive l'option WPS[4]. En effet, vous devez savoir qu'un clé WEP contient une faille de sécurité et peut être déchiffrée très facilement en quelques secondes, ce qui permettrait à une personne malintentionnée d'utiliser votre connexion pour vous espionner ou commettre des délits, cachée derrière votre identité.

Restrictions horaires wifi

Sur certaines boxes, il est possible de préciser des plages horaires pour autoriser/refuser l'accès à votre connexion wifi, ce qui peut largement aider au contrôle parental part exemple, ou encore éviter que des personnes extérieures tentent de s'y connecter à certaines heures.

Filtrage par appareil

La solution la plus fiable pour sécuriser votre accès Internet est d'autoriser uniquement vos appareils (ordinateurs, téléphones, tablettes, etc..) à s'y connecter, en fonction de leur adresse physique unique (adresse MAC), vous aurez ainsi la garantie qu'aucun appareil extérieur à votre

4http://korben.info/cracker-cle-wpa.html

foyer ne s'y connectera ; ceci est paramétrable dans la partie généralement nommée Réseau. Il vous suffit donc de connecter tous vos appareils pour lesquels vous souhaitez autoriser l'accès Internet puis de les autoriser un par un, et enfin d'activer l'option nommée Filtrage MAC.

Solidité des mots de passe

Protéger l'accès à son ordinateur, sa boîte email ou son compte bancaire en ligne par un mot de passe est une règle de sécurité indispensable mais ne les rendent pas invulnérables pour autant ; il faut bien comprendre que plus de la moitié des mots de passe utilisés sont déchiffrables en quelques minutes, par le biais de logiciels spécialisés qui testent automatiquement tous les mots de dictionnaires, les chiffres et les combinaisons des deux. Il est donc très important de respecter quelques règles élémentaires pour bien les choisir :

Longueur

Lors d'une attaque par force brute, plus votre mot de passe sera long, plus son déchiffrement prendra du temps. Un bon mot de passe doit donc contenir au minimum 8 caractères pour qu'il soit difficilement cassable ; il faudrait en effet 66 ans à une machine spécialisée pour casser un mot de passe de cette longueur.

Choix des mots

Le principe est simple : vous devez absolument éviter tout mot pouvant se trouver dans un dictionnaire, ce qui vous protégera de la quasi totalité des logiciels de craquage. Pour la même raison, éviter aussi les prénoms, les dates de naissance et autres noms d'animaux domestiques. Par exemple, si vous vous appelez ***Marie*** et que vous êtes née le *12/02/1980*, que votre chat se nomme ***Felix*** et que vous utilisez ces données dans votre mot de passe, une de vos connaissances ou un pirate bien informé pourra facilement le deviner, très simplement par le biais des réseaux sociaux ou d'autres de vos profils renseignés sur le web.

Autre point très important, ne **jamais** utiliser votre login comme mot de passe, par exemple votre login est ***Marie***, ne choisissez surtout pas ***Marie*** comme mot de passe.

Évitez encore les mots de passe les plus courants tels que **123456**, **abcdef**, **azerty**, **qsdfgh**, **wxcvbn**, **password**, **secret**, **internet**, **admin**, **root**, etc. Ils sont présents dans tous les dictionnaires des logiciels spécialisés et votre mot de passe sera donc cassé en quelques secondes. Certains dictionnaires sont aussi spécialisés dans la recherche de mots juxtaposés, proscrivez donc les mots de passe tels que *l**eslacsduconnemara***.

Invisibilité

Votre mot de passe est personnel et confidentiel et ne dois en aucun cas être partagé, même avec une personne de confiance, car en cas de piratage vous n'aimeriez pas soupçonner un ami. Pour qu'il ne soit pas découvert, ne le stockez nulle part et surtout pas sur un post-it collé sur votre bureau, votre écran ou votre clavier ; encore moins dans fichier informatique sur votre ordinateur.

Création

Maintenant que vous savez pourquoi les mots standards doivent être proscrits, il vous est simple de comprendre que v**ous devez utilisez un mélange de lettres, de chiffres et de caractères spéciaux pour obtenir un mot de passe solide**. Pour exemple, il sera très difficile de casser un mot de passe tel que **j3q!n+81**. Cependant, comme vous pouvez le voir, vous risquez d'avoir du mal à vous en souvenir surtout si vous le notez nulle part ! Hors un mot de passe doit être facile à retenir mais difficile à deviner, il existe donc des solutions pour créer des mots de passe complexes mais facilement mémorisables.

Une solution très efficace : choisir une phrase que vous connaissez parfaitement telle qu'*un vers de poème*, *une citation d'auteur* ou *le titre d'un film* ; prenez ensuite **les premières lettres et le nombre de lettres de chaque mot pour composer votre mot de passe**. Prenons par exemple le titre du film *Et au milieu coule une rivière*. Nous prenons donc les premières lettres de chaque mot : **Eamcur**, puis le nombre de lettres qui composent chaque mot : **226537**. Nous obtenons ainsi le mot de passe suivant : **Eamcur226537**, auquel nous pouvons ajouter divers caractères spéciaux tels que **%**, **+**, **!**, **/**, etc.. Vous pouvez donc jouez au besoin avec ces divers éléments, rendre votre mot de passe plus complexe en alternant **majuscules**, **minuscules**, **chiffres** et **caractères spéciaux**. Exemple de mot de passe sûr composé avec les éléments ci-dessus: **E2%a2!M6+c5/U3$r7**.

Modification

On ne choisit pas un mot de passe pour la vie, il est vivement recommandé de **le modifier régulièrement**. Dans le cas où il serait dévoilé, une personne malveillante ne pourrait pas l'utiliser très longtemps. Il est donc aussi très important de surveiller régulièrement vos emails, qui vous préviennent parfois d'une tentative d'intrusion sur un de vos comptes utilisateurs en ligne, et vous invitent à modifier votre mot de passe. Cependant soyez très vigilants, imitant ce principe, de nombreux emails frauduleux appelés d'hameçonnage sont transmis par des personnes malintentionnées dans le but de vous dérober vos mots de passe et/ou vos données personnelles (voir ci-après).

Hameçonnage

L'***hameçonnage*** (ou ***phishing***) est une technique frauduleuse utilisée pour obtenir des données personnelles dans le but de perpétrer une usurpation d'identité. Elle consiste typiquement à envoyer à des victimes potentielles, des emails semblant provenir de sociétés dignes de confiance (banque, administration, fournisseur d'accès, réseaux sociaux, marchés, etc..) et formulés de manière à inquiéter le destinataire afin qu'il effectue une action précise.

L'approche la plus utilisée étant de vous faire croire que votre compte utilisateur a été désactivé ou qu'il a subi une tentative d'intrusion et que vous devez absolument cliquer sur un lien fourni dans l'email pour vous connecter sur votre compte afin de régler le problème. Ce lien vous dirige alors vers une page web falsifiée ressemblant à vous y méprendre à celle du vrai site de la société en question, puis vous êtes invité à y entrer vos informations confidentielles (identifiant, mot de passe, date de naissance, etc..) qui sont alors enregistrées puis transmises automatiquement au fraudeur.

Pour éviter ce type de fraude, la prudence est de mise, vous devez toujours vérifier :

- que l'orthographe du nom de domaine affiché dans l'URL du lien contenu dans l'email est bien la même que celle du site officiel (exemple : http://naga44.org/).
- que l'URL du lien contenu dans l'email ne contient pas d'arobase (@).
- que l'URL du lien contenu dans l'email ne contient pas de caractères Unicode, placez votre curseur sur le lien puis vérifier l'adresse web en bas à gauche de l'écran.
- que les certificats électroniques sont bien valides (pointer le petit cadenas à gauche de l'URL dans la barre d'adresse du navigateur.

Il est aussi très important de savoir que tous les sites internet bancaires ou marchands utilisent aujourd'hui des certificats électroniques fiables qui permettent de vérifier leur authenticité et qu'ils ne communiquent jamais par email pour corriger un problème de sécurité avec leurs clients. Si vous recevez et détectez un email frauduleux de ce type, n'hésitez pas à le faire suivre à la société concernée, ceci lui permettra d'enquêter et de faire bloquer les pages falsifiées par les autorités.

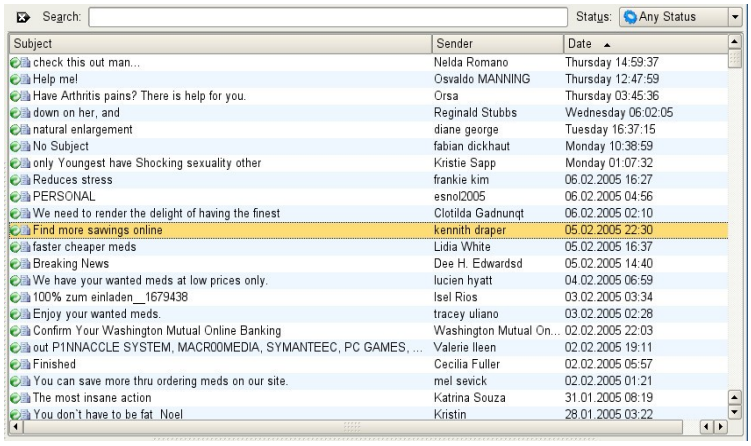
Notez qu'il est vivement recommandé d'écrire manuellement les URL vous-même dans la barre d'adresse de votre navigateur ou d'utiliser vos propres raccourcis plutôt que de cliquer aveuglement sur les liens que l'on vous propose dans vos emails.

Les filtres anti-spam sont aussi une très bonne parade contre ce genre d'emails frauduleux, par exemple le client de messagerie libre Mozilla Thunderbird comporte un filtre bayésien performant et permet de bloquer directement ces emails avant qu'ils n'atterrissent dans votre boîte.

Pour aider les internautes à se protéger contre ce type de fraudes, l'association à but non lucratif Phishing initiative a été créée en 2010 et permet à chacun de signaler les sites web frauduleux francophones en vue de les faire bloquer.

Courriel indésirable

Le courriel indésirable (ou spam) constitue plus de 90 % des courriels transitant sur internet. Il s'agit de l'envoi massif de courriers électroniques non sollicités, manœuvre très rentable qui permet, de façon peu coûteuse, de prospecter massivement de nouveaux clients, proposant majoritairement des arnaques en tout genre tels des remèdes et autres produits pharmaceutiques miracles, des moyens de gagner de l'argent facilement ou encore des biens de luxe à prix cassés.



Bien que souvent très alléchantes, répondre à ces arnaques ne fera que confirmer votre adresse courriel et entraînera immédiatement l'envoi d'autres propositions du même ordre, jusqu'à saturer complètement votre boite courriel. Il faut donc être vigilant et ne jamais y répondre.

En France, le spam est réglementé, d'autant plus qu'il implique la possession, la conservation (et souvent le commerce) de listes d'adresses électroniques récupérées automatiquement (dans des forums de discussion, des sites Web), ce en contradiction avec la loi informatique et libertés.

Théoriquement, une loi impose l'accord des destinataires pour tout type d'envois comportant le nom d'une personne physique. Dans la pratique, les entreprises pratiquant ce genre de commerce ont des réponses types pour se déresponsabiliser : soit l'utilisateur a cliqué par erreur sur un bouton, soit il n'a pas répondu comme il le fallait a une question, ou la liste a été louée à X ou Y.

Dans la loi française, le fait d'envoyer du spam vers une personne morale (une société ou une association par exemple) n'est pas condamnable.

Pour toutes ces raisons, il est très important de vous protéger du spam est de ne pas communiquer votre adresse courriel en clair sur des sites web, chat ou forums, sans quoi elle a de fortes chances d'y être récupérée et diffusée (ou revendue) dans le but d'être spammée. Ne la communiquez uniquement qu'à des gens de confiance tels que votre famille et vos proches.

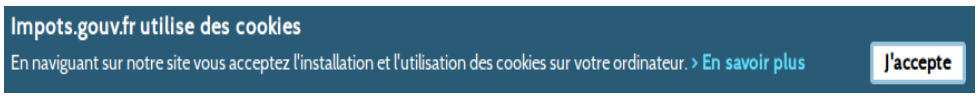
Aujourd'hui, la plupart des fournisseurs de boite courriel proposent de base un système anti-spam intégré permettant de bloquer un grand nombre de courriels indésirables, cependant cela n'est toujours pas suffisant. De plus en plus de fournisseurs proposent donc aussi des filtres personnalisables selon vos besoins, vous pouvez ainsi créer vos propres règles de filtrage et bloquer les courriels contenant des mots-clés précis en entêtes, certaines adresses ou encore un certain type de contenu.

Navigation sécurisée

L'utilisation d'Internet n'a jamais été chose aussi courante qu'aujourd'hui, cependant, aussi pratique que cela puisse l'être, vous devez comprendre que de nombreux risques de sécurité peuvent mettre votre vie privée et votre identité en péril. Il devient alors indispensable à tout internaute, de respecter quelques règles élémentaires pour éviter ces risques.

Cookies

À ne pas confondre avec les biscuits du même nom, les cookies informatiques sont des petits fichiers texte enregistrés sur votre ordinateur par les sites Internet que vous visitez, contenant des informations telles que les dates, heures et durées de vos visites, les versions de votre système d'exploitation (Ubuntu 14.04, Windows 7, etc..) et de votre navigateur (Firefox 38.0, Chrome 45.0, etc..) ou encore l'adresse du site Internet duquel vous provenez.



Ces cookies sont censés faciliter votre navigation lorsque vous retournez sur un site Internet que vous avez déjà visité, cependant leur utilisation reste plus ou moins controversée car il contiennent des informations personnelles pouvant être utilisés par des tiers, bien intentionnés ou non.

De par leur conception, de nombreux sites Internet ne peuvent pas être utilisés correctement sans l'utilisation de cookies, c'est pourquoi vous y voyez fréquemment des messages automatiques vous informant de la nécessité d'autoriser leur utilisation dans votre navigateur (voir plus bas).

Connexions sécurisées

Par défaut, la confidentialité des échanges sur Internet n'est pas garantie puisqu'ils s'effectuent en clair (de manière non chiffrée), s'agissant majoritairement de messages texte, ils peuvent donc être interceptés très facilement par des personnes malintentionnées.

Afin que toutes les informations que vous saisissez sur leurs pages restent privées et sécurisées, certains sites web utilisent SSL (ou *TLS*), protocoles de sécurisation des échanges sur internet.

Lorsque c'est le cas, vous pouvez le vérifier facilement en observant la barre d'adresse de votre navigateur ; le début de l'adresse du site contient alors le protocole HTTPS (avec un S pour Secured) au lieu de *HTTP* ; un petit cadenas apparaît alors à sa gauche comme ci-dessous :

Si vous effectuez des démarches importantes, des transactions bancaires ou autres achats sur internet, il est vivement recommandé de n'utiliser que des sites web proposant le HTTPS.

Moteurs de recherche

Passage incontournable de notre utilisation d'internet, les moteurs de recherche (*Google*, *Yahoo*, etc..) sont un formidable outil de traçage permettant aux entreprises qui les gèrent de se faire une idée très précise de vos centres d'intérêts, des sites que vous fréquentez, de votre avis politique, des actions que vous entreprenez ou encore de votre localisation géographique. Toutes ces données leur permettant de faire aisément ce qu'on appelle du marketing ciblé, voir pire.

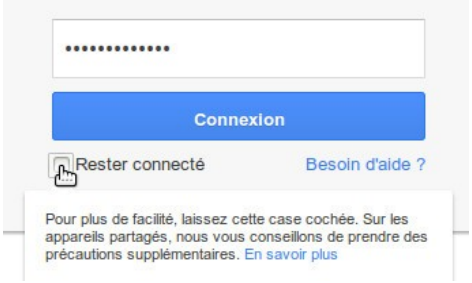
Lorsque vous surfez sur internet, vous êtes identifiable par votre adresse IP, un numéro d'identification unique attribué de façon provisoire ou permanente à chaque appareil connecté à un réseau informatique utilisant l'*Internet protocol*. Cette adresse vous est attribuée par les serveurs de votre FAI. Les moteurs de recherche, tout comme votre FAI, peuvent alors retracer très facilement toute votre activité sur le web.

Pour parer ce problème, il existe des moteurs de recherche tels que Ixquick qui n'enregistrent ni vos recherches ni votre *adresse IP*, votre navigation est alors relativement anonymisée et sécurisée.

Comptes utilisateur

Vous connecter sur vos divers comptes utilisateur sur internet (exemple *Google* ou *Facebook*) n'a rien de très compliqué. Dans la majorité des cas, il vous suffit de préciser votre identifiant (*login*) puis votre mot de passe (*password*) et vous voilà connecté à vos services. Cependant, certains risques de sécurité liés à ces connexions ne doivent pas être pris à la légère.

En effet, la plupart des sites internet où vous êtes inscrit proposent, lors de la connexion à votre compte utilisateur, de cocher une case dans le but de ***Rester connecté***, ce qui signifie que votre navigateur internet enregistrera **votre identifiant et votre mot de passe** dans un cookie afin d'éviter de devoir les entrer de nouveau lors de votre prochaine visite. Ces données resteront enregistrées tant que vous n'aurez pas supprimé les *cookies* de votre navigateur, n'importe quelle personne utilisant votre ordinateur pourra alors accéder librement à ces mêmes comptes.



Si vous êtes la seule personne à utiliser votre ordinateur, cela ne pose pas de problème de sécurité mais si vous êtes dans le cadre d'une utilisation partagée (ordinateur familial ou public), il est vivement recommandé de ne **jamais cocher** cette fameuse case.

Il est aussi très important de comprendre, qu'il s'agisse d'un site banal ou important, d'un chat, d'un forum, d'un réseau social ou d'un jeu en ligne, qu'un compte utilisateur est personnel et qu'il ne dois en aucun cas être partagé par plusieurs personnes. Les conséquences d'une usurpation d'identité peuvent engendrer de sérieux problèmes et vous nuire de manière irréversible.

Afin de garantir votre anonymat, il est vivement recommandé de n'utiliser vos nom et prénom ainsi que vos coordonnées postales et téléphoniques **que lorsque cela est vraiment necésaire**.

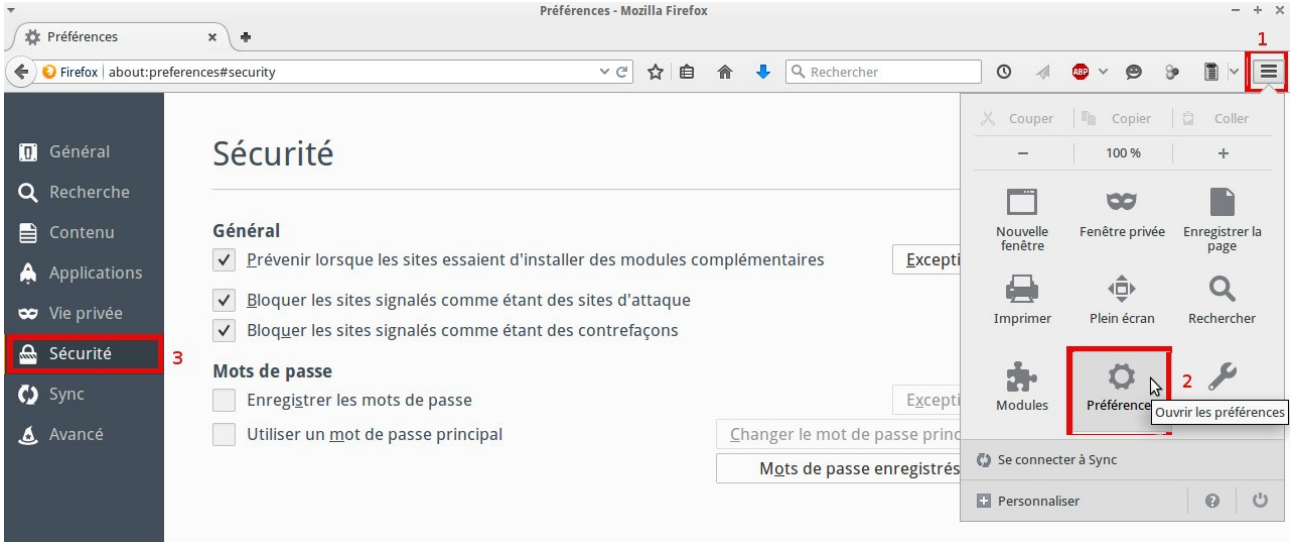
En France, grâce à la loi ***Informatique et Libertés***, vous disposez légalement des ***droits d'accès***, **de rectification**, **d'opposition**, **de déréférencement et de suppression** de vos données personnelles déposées sur Internet. Consultez le site de la CNIL pour exercer vos droits.

Paramétrage du navigateur

Votre navigateur Internet (*Mozilla Firefox*, *Chrome*, *Internet Explorer*, *Opera*) propose généralement par défaut, d'enregistrer vos données de connexion à vos comptes utilisateur, l'historique des sites web que vous avez visité et des fichiers que vous avez téléchargé ou encore les données que

vous avez entré dans des formulaires en ligne.

Peut importe les réglages d'origine de votre navigateur, vous pouvez tout à fait les modifier à votre convenance dans le but de garantir une meilleure sécurité, en vous rendant dans ses *Paramètres* (*options*, ou *préférences*). Il suffit généralement d'y trouver le menu (ou onglet) nommé *Sécurité*, puis selon l'exemple ci-dessous, de cocher/décocher les cases souhaitées.

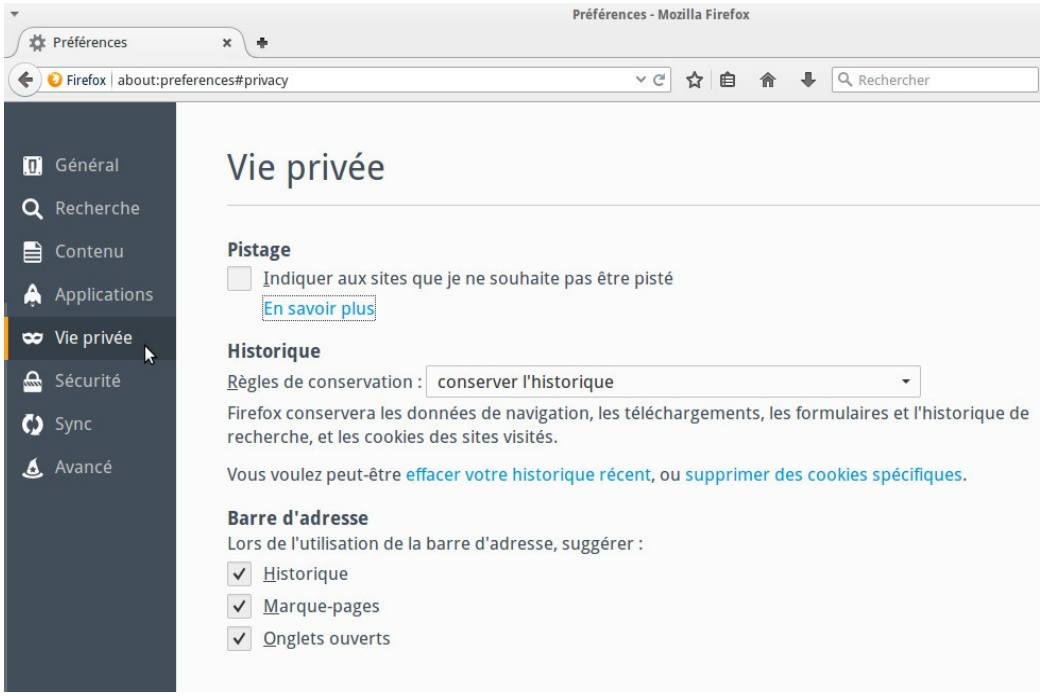


Dans l'exemple ci-dessus concernant le navigateur Mozilla Firefox, il est donc recommandé de **décocher** *Enregistrer les mots de passe* sauf si vous souhaitez *Utiliser un mot de passe principal*, puis de cocher les cases situées dans la partie *Général*. Il est également possible de préciser des exceptions pour certains sites web.

Si vous préférez enregistrer tous vos mots de passe, il est très important d'utiliser un mot de passe principal afin de restreindre l'accès à la liste de vos mots de passe enregistrés. Ils seront ainsi bien gardés si une autre personne que vous utilise votre ordinateur.

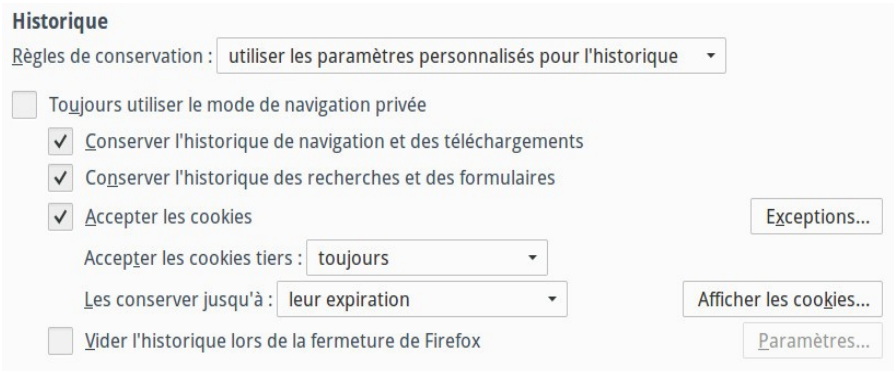
Si la case *Enregistrer les mots de passe* est cochée, votre navigateur vous demandera si vous souhaitez enregistrer vos mots de passe à chaque nouvelle connexion sur vos comptes utilisateur (par exemple sur le site Internet de votre banque, sur *Google*, etc..). Tant que vous ne supprimerez pas les *cookies*, vous n'aurez alors plus besoin de retaper vos identifiants et mots de passe pour vous reconnecter sur les sites où vous les avez déjà enregistrés. Ce qui peut poser problème si quelqu'un d'autre que vous utilise votre ordinateur.

Il est aussi important de paramétrer l'onglet *Vie privée* des préférences de votre navigateur. En général, celui-ci détermine la façon dont l'historique de votre navigation sera conservé, c'est dire si vous souhaitez que votre navigateur enregistre les adresses de tous les sites Internet que vous visitez, toutes vos recherches, tous les fichiers que vous téléchargez ainsi que toutes les données que vous entrez dans les formulaires en ligne, afin de pouvoir les réutiliser ultérieurement.



Certains sites web enregistrent diverses données lorsque vous les visitez, tels que la version du système d'exploitation que vous utilisez (*Ubuntu*, *Windows*, *Mac OS*, etc..), mais aussi le ou les site(s) que vous avez visité juste avant ; il est donc important de cocher la case de ***Pistage***.

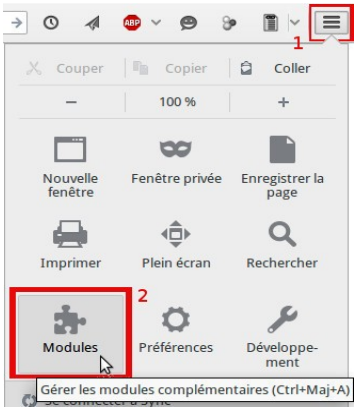
Comme vous pouvez le voir ci-dessus, votre navigateur internet conserve cet historique par défaut, ce qui pose un problème de confidentialité si l'utilisation de votre ordinateur est partagée. Vous pouvez cependant choisir de ne pas le conserver ou encore préciser ce que vous souhaitez sauvegarder et pour quelle durée :



Comme pour l'onglet ***Sécurité*** que nous avons vu plus haut, vous pouvez préciser des exceptions concernant la conservation de cet historique pour certains sites web. Dans tous les cas, il est recommandé de vider votre historique régulièrement pour garantir une bonne sécurité.

C'est aussi dans la partie ***Historique*** que vous pouvez choisir d'autoriser ou de refuser les *cookies* et de fixer leur délais de conservation. Vous pouvez également les afficher pour supprimer ceux que vous souhaitez uniquement.

Dans le but de renforcer la sécurité de navigation, il existe aussi de nombreux modules (ou extensions) variés pouvant être installées sur les navigateurs internet d'aujourd'hui. Certains sont spécialement conçus pour bloquer les fenêtres publicitaires intempestives alors que d'autres seront un outil puissant de contrôle parental, en vous permettant par exemple de créer vos propres filtres, listes blanches et noires. Pour les installer, il vous suffit de vous rendre dans la partie généralement nommé ***Modules*** de votre navigateur internet ; exemple ci-contre avec *Mozilla Firefox*.

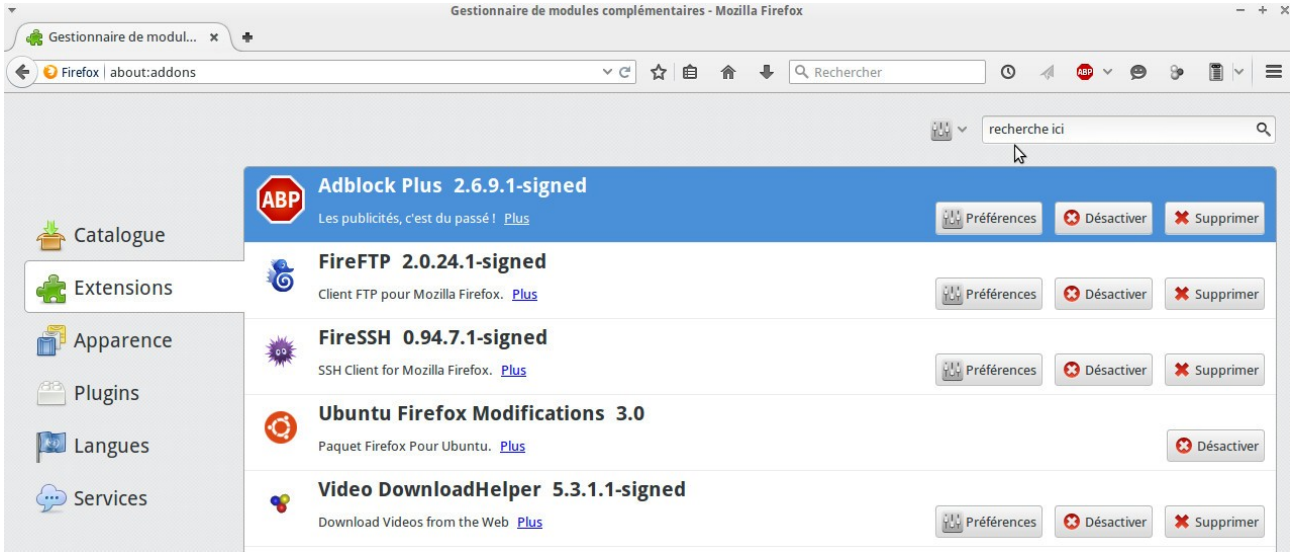


Dans la partie dédiée aux modules, il vous suffit d'entrer le nom du module souhaité si vous le connaissez, ou d'effectuer directement une recherche dans le catalogue par mots clés, puis de cliquer sur le bouton installer ; un redémarrage du navigateur est généralement nécessaire.

Voici quelques modules incontournables de sécurité dont l'efficacité n'est plus à prouver :

- *Adblock Plus* : bloquer les fenêtres publicitaires intempestives et récalcitrantes.
- *FoxFilter* : contrôle parental par le biais de filtres puissants.
- *BlockSite* : bloquer les sites web de votre choix et les liens les reliant.
- *NoScript* : bloquer les contenus exécutables malveillants en Java, Flash, etc..
- *ProCon Latte Content Filter* : bloquer les sites violents et pornographiques.
- *CensureBlock* : bloquer les sites à caractère pornographique.
- *SafeDownload* : scanner les fichiers téléchargés avec plusieurs antivirus.
- *KeyScrambler Personal* : se protéger des codes malveillants de type keylogger.
- *ShowIP* : vérifier l'adresse IP et l'identité d'un site web (contre l'hameçonnage).
- *Flashblock* : bloquer les animations Flash à la volée.

Une fois installés, vous pouvez généralement modifier les paramètres des modules par les boutons ***Préférences***, les ***Désactiver*** en cas de conflit entre plusieurs modules ou les ***Supprimer***.



Pare-feu

Dans le contexte d'un réseau informatique, un ***pare-feu*** (ou ***firewall***) est un composant essentiel de sécurité. Son but est de protéger les ordinateurs connectés au réseau des intrusions indésirables, en filtrant les communications autorisées ou non; par exemple celles entre votre réseau privé domestique et le réseau internet, selon les règles de sécurité que vous aurez paramétré. On peut le comparer à un garde frontière qui autorise ou non un voyageur à entrer dans un pays.

Un pare-feu se présente essentiellement sous deux formes :

- ***logicielle*** : programme installé sur un ordinateur (Gufw par exemple).
- ***matérielle*** : composant physique d'un réseau (*box*) incluant un programme de pare-feu.

Aujourd'hui, la majorité des réseaux domestiques sont reliés à Internet par une *box* (ou routeur) incluant de base un module de pare-feu. Généralement activé d'office, vous devez cependant parfois l'activer par le biais de l'interface de gestion de votre *box* s'il ne l'est pas.

Si vous utilisez un système GNU/Linux, il est alors quasi inutile[5] d'activer le logiciel de pare-feu installé de base (Netfilter), puisque celui de votre *box* garantit déjà une sécurité suffisante et qu'il rend votre ordinateur techniquement inaccessible directement depuis l'Internet. Puis comme nous l'avons déjà expliqué précédemment, quasi aucun service réseau n'est ouvert dans le système *Ubuntu* (par exemple) dans sa configuration initiale.

Par contre, si votre ordinateur est directement relié à un modem téléphonique bas débit ou à un modem *ADSL* classique, si vous utilisez une clé d'Internet mobile ou votre téléphone cellulaire, il est conseillé d'installer un logiciel de pare-feu pour garantir une bonne sécurité et éviter les intrusions.

5 http://forum.ubuntu-fr.org/viewtopic.php?id=399418

Dans un contexte de travail ou lorsque vous vous connectez sur un réseau public (entreprise, association, université, bibliothèque, etc..) depuis un poste de travail mobile (ordinateur portable, tablette, téléphone mobile), il est vivement recommandé d'y installer un logiciel de pare-feu dans le but d'éviter les intrusions provenant de l'intérieur (autres appareils connectés à ce même réseau).

Outils d'analyse et de sécurité

Si vous souhaitez contrôler la sécurité de votre ordinateur sous GNU/Linux, il existe divers outils d'analyse très performants, que l'on peut utiliser facilement et conjointement.

scanner de rootkit : http://www.chkrootkit.org/ ou via la logithèque chkrootkit.

signaler un site de phishing : http://phishing-initiative.com/.

paramétrer son pare-feu : http://gufw.org/ ou via la logithèque Gufw.

tester son pare-feu : http://www.zebulon.fr/outils/scanports/test-securite.php.

tester ses mots de passe : http://assiste.com/Mots_de_passe_Test_de_solidite.html.

gérer ses mots de passe : https://www.keepassx.org/ ou via la logithèque Keepassx.

Supports pédagogiques

Tutoriaux

Vous pouvez trouver différents tutoriels à l'adresse : http://www.asso-linux.org/-Tutoriaux-.

Forum

Si des points ne sont pas abordés pendant la formation ou dans les vidéos, vous pouvez poser des questions sur le forum de Nâga : http://www.naga44.org/forum/.

Remerciements

Remerciements aux contributeurs de la communauté Wikipédia.

Ce support est actuellement incomplet. Vous pouvez nous contacter pour participer à se rédaction/complétion. Merci de votre compréhension.