Sécurité

et

Vie privée

Sommaire

Introduction

Définition :
https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information
La sécurité des systèmes d'informations. Tous les moyens (techniques, organisationnels, juridiques) pour que le système informatique soit disponible dans de bonnes conditions, qu'il ne soit pas détourner de ses buts ou utilisé par des personnes non autorisés.

Évaluer les risques (intrusion, piratage...), rechercher les bonnes protections (accès physique aux machines...), les mettre en œuvre et vérifier leur efficacité (surveiller en temps réel ce qui se passe sur les machines et le réseaux).

Les organismes en France :
ANSSI : Agence nationale de la sécurité des systèmes d'informations : https://www.ssi.gouv.fr/
MOOC : https://secnumacademie.gouv.fr/
CLUSIF : Club de la sécurité de l'information français : https://clusif.fr/
https://www.linformaticien.com/actualites/id/51362/facheux-incident-de-securite-au-clusif.aspx
CERT-FR : Centre gouvernementale de veille, d'alerte et de réponse aux attaques informatiques : https://www.cert.ssi.gouv.fr/

La CNIL : https://www.cnil.fr/
Le RGPD : https://www.economie.gouv.fr/entreprises/reglement-general-sur-protection-des-donnees-rgpd
Le Règlement Général de Protection des données, texte réglementaire européen.

Guide de l'ANSSI :
https://www.ssi.gouv.fr/administration/bonnes-pratiques/

Bonnes pratiques

- mot de passe fort, minuscule, majuscule, chiffre, lettre, caractères spéciaux. Un mot de passe par site. Utiliser un gestionnaire de mot de passe (https://keepass.info/index.html). Pas de mots du dictionnaire, date de naissance. Phrase de passe.

- activer et vérifier le firewall.

- pas d'informations personnelles sur les réseaux sociaux.

- pas ouvrir mail expéditeur inconnu.

- MaJ du système et des logiciels.

- faire attention à ce qu'on télécharge (logiciels sur site officiel).

Md5sum : http://cdimage.ubuntu.com/releases/18.04.2/release/MD5SUMS

http://www.winmd5.com/

https://www.commentcamarche.net/faq/41-md5sum-verifier-l-integrite-des-telechargements

- faire des sauvegardes régulières, divers supports, divers lieux.

- ne pas données d'informations de comptes/bancaire via un simple mail. Vérifier l'adresse du site, du mail.

- modifications régulières du mot de passe.

- antivirus à jour.

- chiffrer ses données, avec GPG4win par exemple :

https://www.gpg4win.org/

- utilisation de BleachBit pour nettoyer régulièrement son ordinateur des fichiers inutiles :

https://www.bleachbit.org/

- effacer ses fichiers de façon sécurisées :

https://eraser.heidi.ie/

Principales menaces

attaques passives (écoute) ou actives (modification, intrusion…).

- *virus* : logiciel malveillant, souvent caché dans un logiciel légitime, qui vise à nuire à un système informatique.
- *vers* : logiciel malveillant qui se répand sur les réseau souvent via la messagerie.
- *cheval de troie*, *trojan*, logiciel malveillant, client serveur, qui permet de prendre le contrôle à distance d'un ordinateur.
- *pourriel*, *spam*, mail indésirable.
- *phishing*, *hameçonnage*, courriel frauduleux imitant un site réel pour tenter de récupérer des informations sensibles.
- Attaque Ddos, déni de service.
A l'aide de machine zombies, infectées (pc, objets connectés…), on sature un serveur en envoyant beaucoup de requête jusqu'à ce qu'il ne puisse plus répondre et devienne donc inaccessible.
Logiciel HOIC, High Orbit Ion Cannon) : https://sourceforge.net/projects/high-orbit-ion-cannon/
- *rançongiciel*, *ransomware*. Chiffrer les données sur un système et demander une rançon pour les déchiffrer.
- *typosquattage*, nom de domaine très ressemblant, pour voler les données des utilisateurs.
- *spyware*, logiciel visant à espionner les activités sur un système, frappes clavier, etc.
- attaque par brute force (John the ripper : https://www.openwall.com/john/). Le logiciel essaye de ″ deviner ″ le mot de passe en se basant sur ceux souvent utilisés.

Sur internet

Dès que l'on va sur internet, on transmet des informations. Tout d'abord, sur notre ordinateur, le navigateur internet enregistre tous les sites que l'on visite, ainsi que les éventuels mots de passe dont on se sert.

En ligne, notre fournisseur d'accès internet enregistre tout ce que l'on fait, chaque page vue. Les sites que nous visitons enregistrent sur notre ordinateur des cookies, qui sont de petits fichiers textes contenant diverses informations, afin de savoir ce que l'on regarde sur leur site et de nous reconnaître la prochaine fois. Et ces cookies peuvent rester sur notre ordinateur pendant plusieurs années si l'on n'y prend pas garde. Dans Firefox, allez dans le menu « *Outils* », puis « *Options* » et dans l'onglet « *Vie privée* » regardez les cookies stockés sur votre ordinateur.

Et notre navigateur internet donne également des informations sur notre ordinateur, sa configuration et sa localisation. Rendez-vous sur ce site, puis allez dans la rubrique « *Vos traces* » dans le menu de gauche.

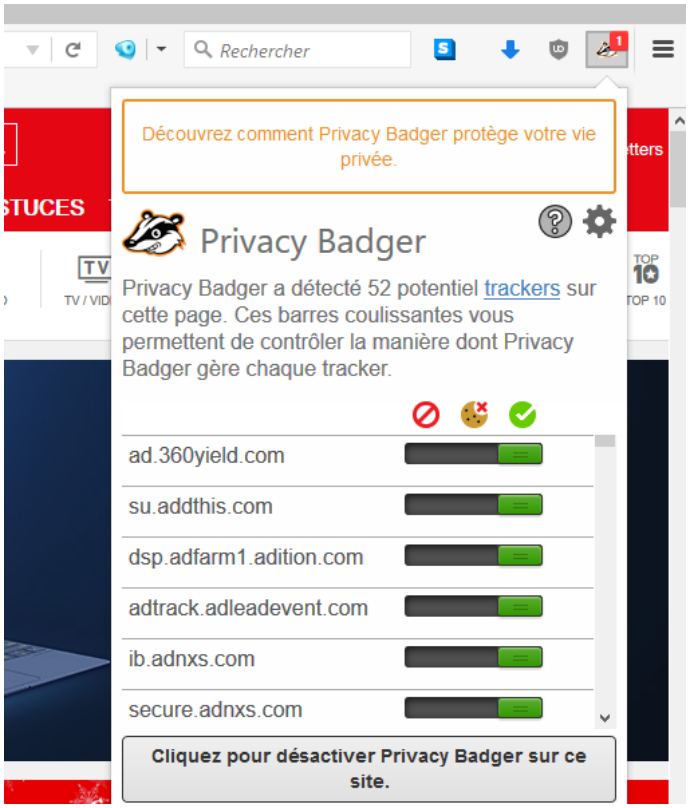
Le pistage

Les sites commerciaux, ainsi que les réseaux sociaux, sont très friands d'informations sur leurs visiteurs. Ils ont donc développé des techniques pour nous suivre, savoir ce que l'on visite, quand, comment. Grâce au recueil de ces informations, ils peuvent ensuite nous proposer des publicités ciblées, directement en rapport avec nos envies. Ces grosses sociétés peuvent savoir si l'on passe du temps sur des sites de jardinage, de téléphones portables, et puis, ensuite, on reçoit des mails de société de jardinage, ou de téléphones portables, et dans Google des publicités traitant de ces sujets là apparaissent lors de nos recherches. Une solution peut consister à utiliser le moteur de recherche Qwant. Il n’enregistre pas les données des utilisateurs et affiche les même résultats pour tout le monde.

Comme sur les réseaux sociaux, toutes les informations que l'on donne volontairement ou non, sont enregistrées, analysées, partagées puis utilisées pour essayer de nous faire acheter certains produits qui pourraient nous intéresser. Tout cela sans que l'on ne demande rien, sans nous demander notre avis, ni même souvent sans qu'on le sache.

Le module Kimetrak pour Firefox permet de vous montrer avec quels sites communiquent le site que vous visitez.

Voici un exemple avec Privacy Badger sur un site de logiciels informatique. Il y détecte pas moins de 52 trackers potentiels.



Les mails

Lorsque l'on envoie un mail, un certain nombre d'informations sont envoyées avec, comme les adresses IP des serveurs de courrier par lesquels transite le mail, le logiciel (et sa version) utilisé pour écrire le mail, l'hébergeur de l'expéditeur. On peut assez facilement géolocaliser quelqu'un qui nous a envoyé un mail (il y a des sites spécialisés sur internet).

Et en plus, certains fournisseurs de mail, comme Yahoo ou Gmail, font lire vos mails à des logiciels afin d'y détecter certains mots clés pour savoir quelles publicités vous envoyer.

Sans parler de certaines agences de renseignements Américaines qui peuvent intercepter des millions de communications électroniques par jour pour lutter contre le terrorisme (système Echelon par exemple, ou PRISM).

Comment se protéger

Sur internet

Si l'on souhaite protéger sa vie privée sur internet, il y a déjà une chose simple à faire : ne pas donner d'informations personnelles sur les réseaux sociaux, les forums et les chats. Cela parait évident, et pourtant... Il faut maîtriser les informations personnelles que l'on publie. Pensez également à toujours vous déconnecter des sites sur lesquels vous allez, et ne pas laisser votre session active en fermant simplement le navigateur.

Ensuite, si vous souhaitez pouvoir surfer sans que tout ce que vous fassiez et regardiez sur le net ne soit enregistré, analysé, partagé, re-vendu, il existe des solutions.

Bien sûr, plus vous souhaiterez être libre, plus ces solutions seront contraignantes, c'est un prix à payer pour pouvoir préserver sa vie privée sur internet.

> Firefox, le navigateur libre de la fondation Mozilla, dispose de nombreux plugins pour protéger la vie privée.

Parmi ceux-ci, on peut citer :

uBlock Origin permet de masquer les publicités lorsque vous surfez.

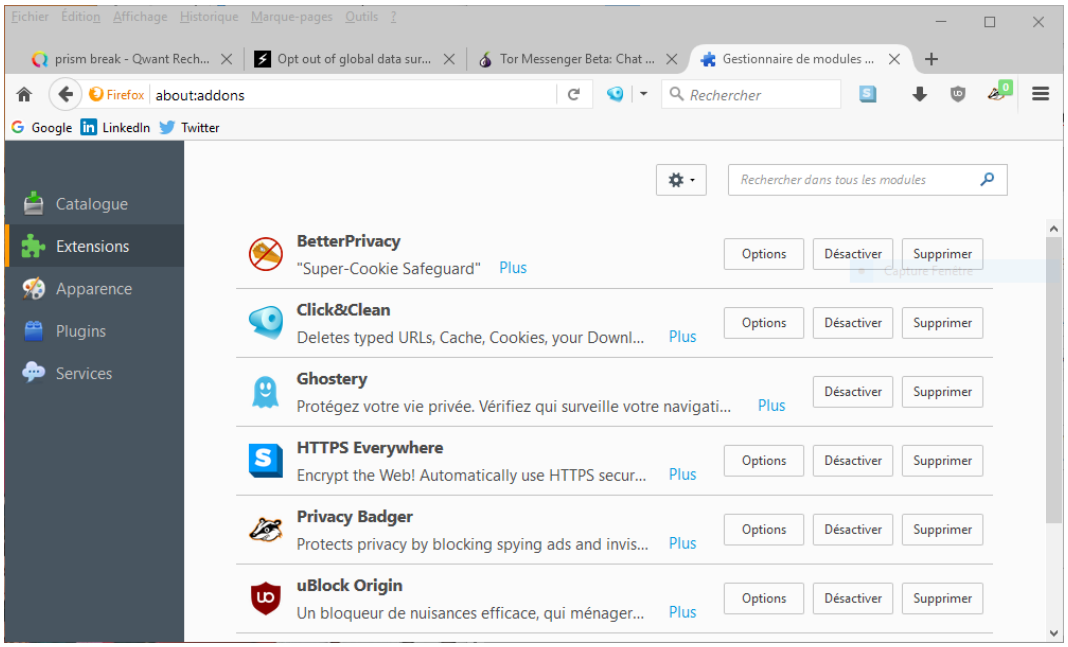
Privacy Badger permet de surveiller et bloquer les services qui vous espionnent.

HTTPS Everywhere, qui est développé par l'EFF, permet, sur les sites le permettant, de se connecter automatiquement en session sécurisée (HTTPS) et donc, les communications sont cryptées.

Il y a également des plugins qui modifient le nom de votre navigateur internet (le user agent), qui vous permettent d'utiliser simplement des proxy (logiciels redirigeant les connections afin de masquer l'origine de la demande) , de gérer finement les cookies.

L'installation de plugins pour Firefox est de plus en plus simple, car maintenant, pour la plupart, il n'y a même plus besoin de re-démarrer.

On va sur la page du plugin, on clic sur « *Ajouter à Firefox* », on accepte que ce site puisse installer des extensions, et c'est terminé. Ensuite, il n'y a plus qu'à configurer le plugin. Pour les gérer, on va dans le menu « *Outils* » puis « *Modules complémentaires* » :

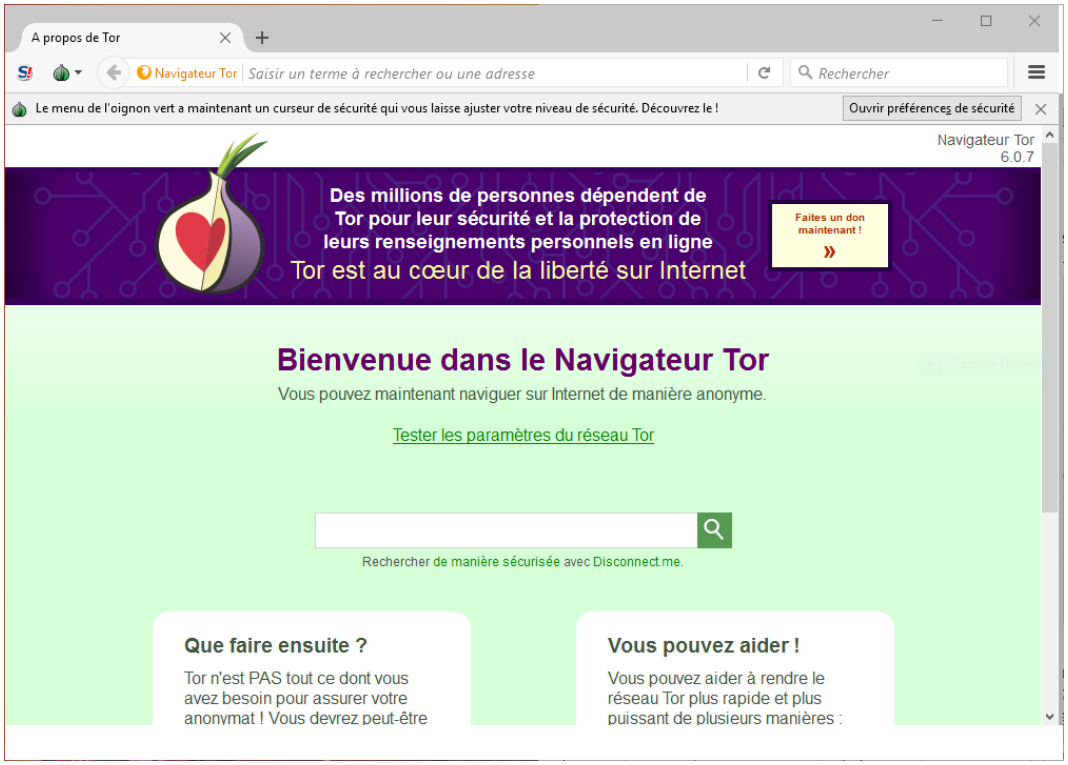


D'autres solutions existes évidemment pour surfer de façon plus discrète :

Utiliser un VPN, réseau privé virtuel, qui permet de sécuriser les échanges réseaux.

Utiliser des proxys.

Mais la solution la plus efficace est le réseau Tor qui est décentralisé et sécurisé. Il suffit de télécharger l'archive Tor Browser Bundle, et de la décompresser. Ensuite, on va dans le répertoire *tor-browser_fr* puis on lance *start-tor-browser.* Une fenêtre s'ouvre, où il n'y a plus qu'à lancer *Tor* :



Et vous voilà avec une version du navigateur Firefox configurée pour utiliser le réseau Tor. Lisez également les Warnings pour utiliser Tor Browse Bundle de façon réellement efficace.

Grâce à ceci, et en suivant les warnings, votre surf sera protégé et vous ne serez pas espionné.

Pour communiquer

Le réseau Freenet, différent d'internet, totalement crypté, décentralisé, permet une liberté d'information et d'expression presque totale, et c'est un logiciel libre. On peut discuter sur des forums et échanger des mails avec d'autres utilisateurs de Freenet de façon anonyme.

Pour les mails, il ne faut jamais répondre si l'on ne connaît pas l'expéditeur (supprimer directement le mail, sans l'ouvrir), et ne surtout pas donner de codes confidentiels, numéros de cartes bancaire ou autres, ni même cliquer sur un lien.

Le phishing, technique consistant à se faire passer pour un organisme officiel, une banque, est le principal risque par mail.

Avoir une adresse mail servant uniquement pour s'inscrire sur des sites, forums ou autres, et une adresse uniquement pour sa famille, ses amis et collègues.

Pour sécuriser ses mails, il existe pour Thunderbird le plugin Enigmail permettant de chiffrer et / ou signer ses mails avec OpenPGP, afin qu'ils ne puissent être lu que par le destinataire.

Une fois le module installé et Thunderbird redémarré, rendez-vous dans le nouveau menu *OpenPGP*, puis lancez *Assistant de configuration*.

Laissez-vous guider par les différentes étapes pour créer vos clés publiques et privées (choix du compte à activer pour OpenPGP, puis création des clés publiques et privées, par défaut d'une validité de 5 ans, de 2048 bits avec le protocole RSA), et créez également un certificat de révocation (utile si vous avez besoin d'annuler votre clé).

Ensuite, vous pouvez, dans le menu *Préférence*s d'OpenPGP, configurer certains paramètres, dont choisir ou non de chiffrer les mails à chaque fois :

Toujours dans le menu d'OpenPGP, vous pouvez également accéder à la *Gestion des clefs / Générer / Nouvelle paire de clefs*, afin de personnaliser vos clefs (date d'expiration, taille de la clé, cryptage utilisé).

Quand vous écrirez un message depuis Thunderbird, depuis le menu *OpenPGP*, vous pourrez choisir de *chiffrer* et / ou *signer* votre mail.

Afin que votre destinataire puisse lire votre message chiffré, il faut mettre la clé publique sur un serveur de clé, comme par exemple *pgp.mit.edu*.

Voilà, vous avez un compte mail qui peut envoyer des mails chiffrés et / ou signés, afin que seul le destinataire puisse les lire, et afin qu'il soit sûr que l'expéditeur est bien celui affiché.

Pour finir

On le voit, les dangers actuels sur le respect de notre vie privée sont réels et importants. Tout le monde est connecté, donc tout le monde peut être espionné. Et les techniques et moyens mis en œuvres sont de plus en plus importants. Donc, il faut réagir, s'informer, et se protéger.

Certaines choses sont simples à mettre en œuvre, et relève simplement du bon sens. Et si l'on veut aller plus loin dans la protection de la vie privée, des techniques existent afin de sécuriser ses communications. Les outils sont là, il suffit d'apprendre à s'en servir et les utiliser à bon escient.

Bien sur, cela complique les choses, et rend le surf moins facile. Mais c'est le prix à payer, aujourd'hui, pour essayer de faire respecter un peu sa vie privée, ce qui est enjeu important.

Le plus grand problème, à mon avis, est surtout le manque d'information, et également de prise de conscience, du public vis à vis de ce problème.

Bibliographie

http://www.bugbrother.com/eff/eff_privacy_top_12.html
http://www.bugbrother.com/archives/sortezcouvert.html
http://www.vie-privee.org/liens/liens.php
http://www.anonymat.org/download.htm
http://linuxmanua.blogspot.fr/2009/03/cyber-resistance-anonyme-en-2-minutes.html
http://www.bugbrother.com/security.tao.ca/intro.html
https://securityinabox.org/fr
https://guide.boum.org/tomes/1_hors_connexions/unepage/
http://www.netpublic.fr/2012/03/proteger-sa-vie-privee-sur-internet/
https://tails.boum.org/
https://prism-break.org/fr/