Aux doigts et à l'œil

l'ordi sobre et lucide du Gard
groupe d'auto-éducation au numérique

Pack de "survie"

Présentation

Cette série a pour but d'aider les nouveaux utilisateurs ou ceux qui n'ont pas le temps de chercher les informations à prendre le moins de risque possible.

Cette démarche va, en apparence, à contre-sens des objectifs de Aux doigts et à l'oeil qui sont de prendre le temps de réfléchir ensemble à des solutions pour chacun plutôt que de donner une hypothétique solution universelle.

Mais si on débute dans l'utilisation d'un ordinateur et/ou d'internet, ou si on n'est pas intéressé par la "technique", on peut mettre son ordinateur en danger juste par manque d'informations.

De plus un ordinateur infecté par un virus peut transmettre ce virus à ses contacts, une boîte mail piratée transforme ses contacts en cibles pour le pirate, un ordinateur envahi de pubs empêche de travailler sur des projets partagés, faire des recherches sur Google exclusivement cache une partie des informations peut-être nécessaires pour une réflexion complète, etc. Étant en constant contact les uns avec les autres, ce qui touche notre ordinateur peut toucher nos contacts, parfois sans même qu'on s'en aperçoive.

Ce "pack de survie" sert donc à aider les nouveaux ou débutants à protéger leurs contacts en protégeant leur propre ordinateur et accès à internet.

Dans ce 1er numéro on aborde les sujets les plus urgents et faciles à régler :
- navigation limitant les traçages par les sites,
- installation sans pubs de logiciels depuis internet,
- recherches sans Google donc anonymes (déjà présent dans la newsletter 1).

I. Navigateur web

1. Téléchargement et installation de modules "de prudence"

Le navigateur nous donne accès à internet, en navigant de page en page, en téléchargeant des fichiers, en écoutant de la musique... c'est un outil, comme une voiture, qui nous permet d'aller "sur internet", comme "sur une autoroute".

Par exemple, Internet Explorer, Google Chrome ou Mozilla Firefox ne sont pas "internet", ce sont des navigateurs, on peut choisir celui qu'on veut.
Le choix du navigateur influence la vitesse de navigation et téléchargement mais aussi le "partage involontaire" de données et d'informations. Même parmi les navigateurs web "open source"*, les produits Google par exemple collectent toutes les données et informations qu'ils peuvent, ça fait partie de leur "business model".
Google Chrome est un produit "open source" de Google, il ne protège donc pas nos données.
Internet Explorer est un produit "propriétaire" de Microsoft, il ne protège pas nos données.

Mozilla Firefox est le plus connu et facile d'utilisation des navigateurs web "libres". Il est téléchargeable :

pour Windows	https://www.mozilla.org/fr/firefox/new/
pour Linux	`# apt-get install firefox`
pour Ubuntu	`$ sudo apt-get install firefox` *`mdp_utilisateur`*

On peut télécharger et installer les modules et extensions depuis le **"menu hamburger"**
(en haut à droite de la page web)

> puis **Modules et extensions**
(ou Add-ons en Anglais, selon les traductions).

ou depuis https://addons.mozilla.org/fr/firefox/.

Quelques modules intéressants :

- **HTTPS-Everywhere** : Utilise le protocole HTTP en mode chiffré (avec SSL) pour se connecter aux pages demandées sur internet.
Les informations envoyées et reçues ne sont pas visibles, car chiffrées, par un "méchant" qui tenterait d'intercepter ce qui est échangé. Ce processus est transparent pour l'utilisateur, le navigateur et les serveurs d'internet font leurs échanges de "clés de chiffrement/déchiffrement" sans qu'on ait besoin de comprendre ce qu'ils font.
https://www.eff.org/https-everywhere

- **Ghostery** : Bloque les mouchards (logiciels espions, statistiques etc.), les cookies des sites publicitaires et les pubs.
https://www.ghostery.com/try-us/download-navigateur-extension/
Avec le succès Ghostery devient plus "clientophile", ce qui signifie qu'il négocie avec certaines entreprises et laissent passer quelques mouchards, pubs et cookies. Un remplaçant serait le bienvenu !

- **uBlock Origin** : Bloqueur de pubs, plus fiable qu'AdBlock Plus.
https://addons.mozilla.org/fr/firefox/addon/ublock-origin/

- **HTML5 Video Everywhere!** : Permet de regarder certaines vidéos en html5 au lieu d'Adobe Flash Player.
https://addons.mozilla.org/en-US/firefox/addon/html5-video-everywhere/
Flash est un logiciel propriétaire d'Adobe, certaines version on été criblées de failles de sécurité. C'est plus prudent d'éviter d'utiliser et d'installer Flash quand on peut, c'est un Plus.

2. Réglages de Firefox

Les réglages se font pour la plupart depuis le **"menu hamburger"**
(en haut à droite de la page web)

> puis **Préférences**.

---

* Dans un prochain article de "aloeil" on expliquera les différences entre "open source" et les licences "libres".

II. Téléchargement de logiciels depuis internet

Pour l'utilisation de notre ordinateur, on a parfois besoin d'un logiciel qui n'est pas installé. On doit l'installer, et la plupart du temps le télécharger depuis internet. L'opération de télécharger un logiciel est sécurisée, mais le logiciel qu'on télécharge peut contenir des surprises.

Ce qu'on télécharge, je l'appelle le "colis 3suisses", parce qu'il contient le logiciel commandé et une flopée de pubs et offres cadeaux comme dans les commandes aux 3suisses.

Plusieurs **intermédiaires** s'occupent du colis entre les développeurs et nous :
- la plateforme d'édition ("forge" en anglais informatique) qui offre des services à certains développeurs,
- les sites d'information technique qui le proposent parfois "gratuitement",
- des sites "aimants" qui n'ont rien à offrir mais tentent de faire télécharger des logiciel purement malveillants,
- et d'autres, tant que l'imagination en trouve.

C'est via ces intermédiaires que les surprises sont insérées, pour cela il est bon de différencier les sites sûrs des sites plus "3suisses" et de ceux qui collectent des données sur les utilisateurs.

1. Les sites "3suisses" (concernant les téléchargements)

Ce sont des sites qui peuvent être très intéressants pour les informations techniques qu'ils diffusent, mais qui insèrent des pubs "obligatoires" dans les logiciels qu'ils proposent. Au final, le logiciel peut bugger du fait d'une mauvaise intégration des pubs, et on doit supporter les pubs (qui elles ne buggent pas). Ces pubs-là ne peuvent pas être enlevées sans trifouiller dans le code du logiciel, il vaut donc mieux éviter de télécharger des logiciels sur ces sites.
Clubic.com, softonic, 01net.com, (à compléter au fur et à mesure des découvertes)

2. Les sites collecteurs de données personnelles

Ces sites utilisent des mouchards (cookies, outils de statistiques) pour tracer quels sites on consulte et ce qui nous intéresse, ils demandent aussi quelquefois de remplir un questionnaire pour télécharger un logiciel.

Pour la plupart, ces sites ne proposent pas de pubs, c'est au moment de la navigation ou du téléchargement qu'ils collectent nos données de navigation. Aucun danger immédiat pour notre ordinateur, on peut très bien télécharger et installer des logiciels venant de là :
sourceforge.net, github.com, (à compléter au fur et à mesure des découvertes)

3. Les sites de confiance

Ces sites sont fiables (pour l'instant). Les logiciels qu'ils proposent sont à jour (la version proposée en téléchargement est la dernière version du logiciel), ils ne mettent pas de pubs à eux dedans et préviennent quand les colis 3suisses peuvent contenir des pubs à l'installation. Ce sont des pubs qui s'installent en même temps que le logiciel mais qu'on peut éviter d'installer (cf III ci-dessous).

Par "sites de confiance", j'entends "sites qui ne posent jusqu'à maintenant pas de problème de sécurité ou de collecte de données. Je n'ai personnellement jamais rencontré de problèmes avec des logiciels téléchargés sur ces sites, ce qui ne veut pas dire qu'il n'y en aura jamais. Sur commentcamarche.net, on peut même leur écrire, si on trouve une mise à jour qu'ils n'ont pas encore mise en ligne par exemple, ils répondent et renseignent.

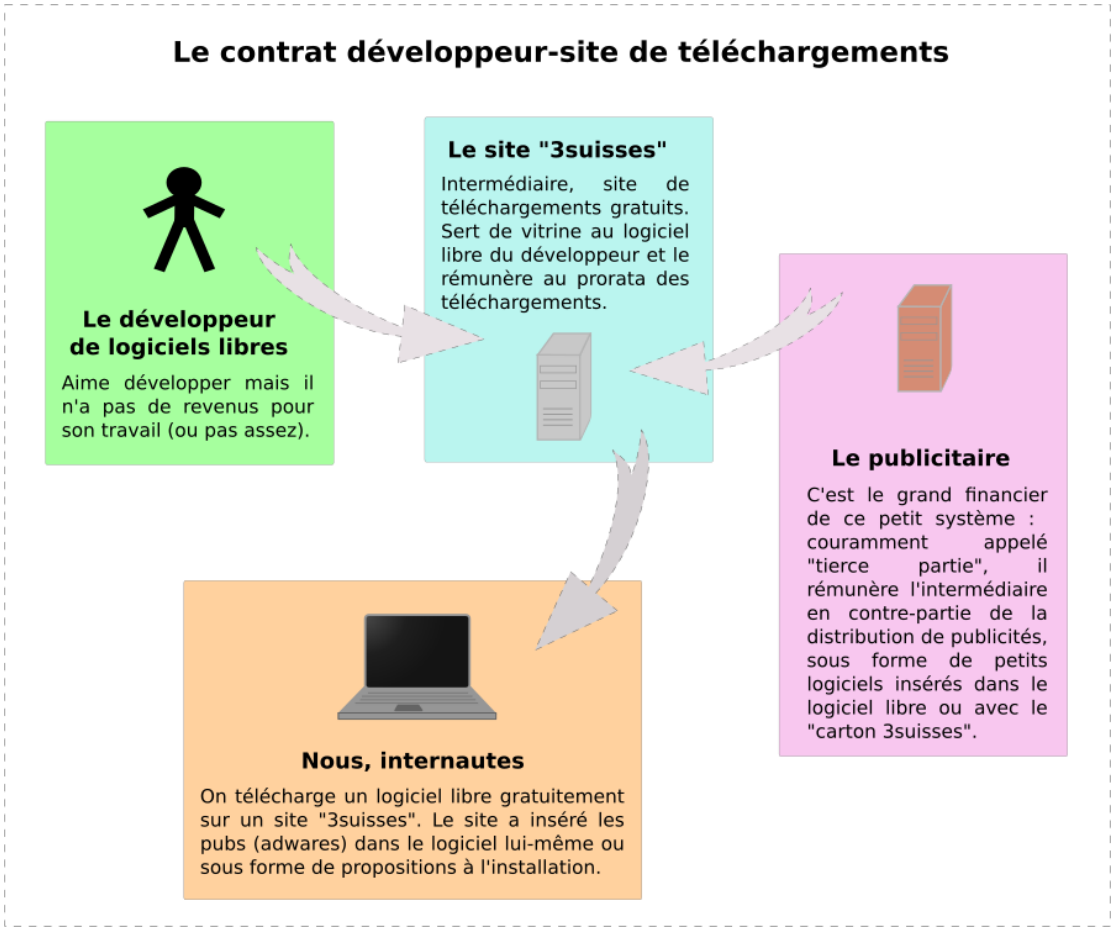
Les sites de confiance sont :
commentcamarche.net, tootlslib.net, filehippo.com/fr.

Les dépôts (repositories) :
github.com, framagit.org etc. proposent pour certains logiciels, de télécharger une archive installable sur Windows (.zip) ou la ligne de commande pour les systèmes GNU/Linux.

III. Installation de logiciels téléchargés depuis internet (Windows)

Les logiciels libres sont souvent gratuits au téléchargement, à l'utilisation, au partage, etc., ce qui fragilise leur développement et leur maintenance : les développeurs doivent travailler en parallèle pour vivre, ça réduit leur temps disponible pour les logiciels libres et gratuits. Pour chaque logiciel libre téléchargé gratuitement, on peut faire un don aux développeurs (bouton "donate"), mais leurs revenus sont jamais suffisants. Certains

développeurs préfèrent compléter ces revenus en signant des contrats avec des entreprises, soit un contrat de travail, soit d'intermédiaire. Dans le cas d'un intermédiaire, des logiciels de publicité (adwares) propriétaires sont insérés dans le logiciel ou le carton "3suisses".



Quand notre ordinateur "rame", que dans l'entête du navigateur on trouve des boutons qu'on n'a pas voulu installer, que le navigateur qui s'ouvre en cliquant sur un lien n'est pas notre navigateur "par défaut", quand la page d'ouverture du navigateur n'est pas la page qu'on avait inscrite dans les préférences... c'est qu'on a installé un logiciel de pub ou adware. Ils sont faits, aussi, pour qu'on ne puisse pas les supprimer en supprimant leur dossier dans "program files", avec une petite astuce qui les réinstalle si on supprime ce dossier !

1. Comment ne pas installer ces adwares ?

Une fois le colis "3suisses" téléchargé, il est "recommandé" par windows de double-cliquer dessus et d'accepter l'installation "standard". L'autre choix est "déconseillé" ou "réservé aux experts", c'est "l'installation personnalisée".
En fait, l'installation standard installe le logiciel le premier sur la liste des "cadeaux gratuits", comme indiqué dans le contrat publicitaire-intermédiaire-développeur.
L'**installation personnalisée** n'installe pas d'office les adwares, elle demande si on veut installer le 1er adware. **Il faut cocher "non merci" ou "non" ou "refuser"**... alors il proposera le 2è adware prévu, qu'il faut refuser, il proposera le 3è, et ainsi de suite, jusqu'à ce qu'il n'en ait plus à proposer et installe le logiciel téléchargé sans les adwares et sans sanction sur la qualité du logiciel.
La technique marketing est de compter sur notre manque de patience et de confiance en nous, plus il en est proposé plus on risque de cliquer "oui". Le plus que j'en ai refusé était 7, donc ne pas se décourager !

2. Comment s'en débarrasser ?

Comme on l'a vu, on ne peut pas simplement supprimer leur dossier dans Program files, Ccleaner est insuffisant aussi et ils ne sont pas détectés par les logiciels anti-virus. Ce ne sont pas des virus à proprement parler, puisqu'ils ne se transmettent pas d'un ordinateur à un autre, et techniquement ne sont pas dangereux : ils ne sont pas faits pour détruire ou abîmer, juste pour nous faire acheter des choses que vendent leurs fabricants.

Pour retirer les adwares, 2 logiciels (libres et gratuits) sont très bons et complémentaires :

Adwcleaner, édité par Xplode, téléchargeable sur Toolslib :
https://toolslib.net/downloads/viewdownload/1-adwcleaner/
et sur commentcamarche :
http://www.commentcamarche.net/download/telecharger-34096208-adwcleaner
Il s'utilise sans installation, en double-cliquant directement sur l'icone du logiciel téléchargé. Quand, après le scan, on demande à Adwcleaner de nettoyer l'ordinateur, il nous engueule et nous dit qu'il faut sortir couvert ; son logo est un morpion :p

Malewarebytes sur commentcamarche :
http://www.commentcamarche.net/download/telecharger-34055379-malwarebytes-anti-malware

Ces 2 logiciels ne traitent pas les mêmes adwares, selon l'adware qui nous embête, on peut être amené à passer les 2.

Les moteurs de recherche alternatifs

Le moteur de recherche est le moyen le plus répandu pour trouver des sites internet ou y accéder.

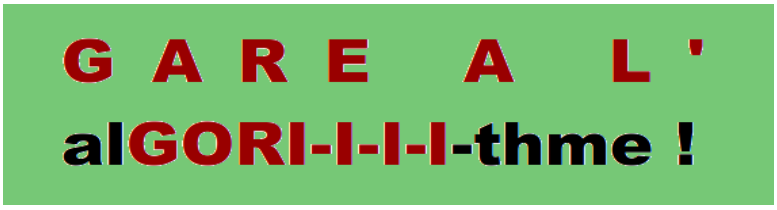
l'aspect écologique

Taper une requête (= une question) sur google c'est déclencher instantanément une armada de "serveurs" connectés entre eux et avec ton ordi. Ce qui consomme à chaque fois de l'énergie directe (électricité) ou encore plus, indirecte (usure des machines).

Si je cherche par exemple "serveur" sur google, j'ai "environ" 32 100 000 résultats (0,53 secondes), ce qui est légèrement déraisonnable. Comme j'avais l'intention de consulter d'abord wikipedia, le plus sobre et lucide est de :
a) ajouter wikipedia à mes favoris
https://fr.wikipedia.org/wiki/Wikipédia:Accueil_principal
b) cliquer dessus.
On arrive ainsi à wikipedia tout de suite sans avoir eu à mettre en branle tous les serveurs du monde pendant 0,53 secondes et on consomme d'après l'ADEME 4 fois moins d'énergie. (voir ADEME 2014
http://www.ademe.fr/sites/default/files/assets/documents/guide-pratique-internet-courriels-reduire-impacts.pdf).

nos "données" nous appartiennent

Tout le monde sait maintenant que nos faits et gestes, nos petits clics et parcours de santé divers sont observés, numérisés et revendus par devers nous aux "entreprises" qui nous renvoient des "offres" commerciales toujours plus abusives, mais les données sont aussi piquées par les agences de renseignement gouvernementales (NSA etc.), par le secteur pharmaceutique, les assurances, les banques, l'EDF, etc. et par le gouvernement via les services de renseignement (cf Loi Renseignement de juillet 2015). Grâce à ces "données" les algorithmes nous attribuent par exemple des cotations personnalisées pour l'attribution d'un prêt bancaire basées sur nos messages facebook et ceux de nos amis, des amis de nos amis, etc. et bien pire encore.



Ce petit jeu d'épicier en données personnelles n'intéresse cependant plus beaucoup Google qui est devenu bien trop riche maintenant pour en rester là, la visée est beaucoup plus ambitieuse, nous sonder en permanence pour transformer l'éducation, les transports, la médecine, et même nous transformer (transhumanisme)... tout cela au nom du progrès, de la productivité, de l'innovation, du bien-être, de la croissance ... Que du bonheur !

Il faut donc y regarder de près. Et, sans prétendre tout régler, chercher à limiter les soucis potentiels, c'est déjà bien.
Il existe des moteurs de recherche qu'on peut utiliser à la place de google, yahoo, facebook, etc. et qui ne retiennent pas nos coordonnées et ne peuvent donc pas transmettre nos données ni nos recherches, et ainsi "ne nourrissent pas le troll" google-Adwords (adwords est la régie de pub de google qui vend les mots-clés aux enchères)
Ce sont les moteurs dits "confidentiels" ou "alternatifs". A l'usage, ils rendent à peu près les mêmes services que google.
Sans entrer dans les détails, on retiendra pour l'instant les moteurs qui sont agréés par des organismes fiables (comme la quadrature du net).

image : Le troll créature monstrueuse peu amicale ou agressive du folklore scandinave wikipedia

les "bulles"

Google utilise aussi nos données d'une autre manière : orienter la réponse à notre question à notre insu, en fonction de nos recherches antérieures et créer ainsi une "personnalisation" appelée "bulles" ou "bulles de filtres" https://fr.wikipedia.org/wiki/Bulle_de_filtres.
Vous pouvez ainsi être enfermé(e)s dans une bulle en croyant recevoir la même information que tout le monde.
Une petite présentation du phénomène des bulles sur le site d'un moteur (duckduckgo) qui se dit confidentiel : http://dontbubble.us/.

"Libérer votre porte d'entrée au Web"...

On peut facilement et sans inconvénients échapper à ce gigantesque fichage en utilisant des moteurs "confidentiels" qui, en brouillant les pistes, empêchent de recueillir nos données. Il en existe beaucoup. On pourrait partir de celui-ci : searx (https://searx.me/)
Moteur utilisé par la "quadrature du net" qui fait référence en matière de confidentialité.
Comme c'est un logiciel libre, il a été adapté ("forké") de nombreuses fois. Framabee (https://framabee.org/) une de ces modifications de searx par l'association framasoft bien connue de nous.
Ce moteur se base sur les interrogations d'autres moteurs comme Google (on peut les choisir dans "préférences") et ne possède donc pas de serveurs en propre (c'est le cas de le dire).
Il ne conserve pas les informations de ses utilisateurs et ne transmet pas les recherches aux autres moteurs.

Comment intégrer ces moteurs dans firefox ?

1) préférences > page d'accueil > https://www.searx.me (facultatif)
2) barre de recherche > paramètres de recherche > ajoutez d'autres moteurs de recherche > searx.me 0.9.x > Ajouter à firefox
3) le faire remonter en haut dans la liste des moteurs de recherche pour y accéder en priorité
Les autres adaptation de searx comme framabee ne figurent pas dans la liste des moteurs pouvant être ajoutés à firefox.