Félix DESMARETZ Paul GOGA
Julia BEROUX Dorian ARCHENAULT
Julien BENATAR Suzanne CAPILLAIRE

Navigation internet

En tant qu'étudiant, il nous faut être informé sur les différents dangers présents sur Internet. Voici une liste de quelques conseils qui vous serviront à protéger vos données lors de vos prochaines expéditions sur le web.

- **Principes de sécurité**

	Conseils	Choses à ne pas faire
Niveau 1	• Utiliser un moteur de recherche offrant plus de transparence • Refuser les **cookies** • Utiliser la navigation privée	• Cocher la case "Rester connecté" • Cliquer sur un lien sans en regarder la cible • Avoir le même mot de passe partout
Niveau 2	• Forcer des connexions cryptées **HTTPS** • Bloquer les **cookies flash** • Désactiver le **Javascipt** • Bloquer les publicités/les **trackers**	• Ouvrir n'importe quel mail et n'importe quelle pièce jointe sans en vérifier l'authenticité
Niveau 3	• Utiliser un **proxy** • Utiliser un **VPN** • Utiliser le réseau **TOR** • Garder les données importantes sur une machine ou un stockage déconnecté de tout réseau	• Communiquer en clair des informations confidentielles/personnelles • Garder des informations en clair sur son disque dur • Dévoiler son identité, même derrière des protections

- **Applications**

Utiliser un moteur de recherche offrant plus de transparence

Google est le navigateur le moins sécurisé et pourtant c'est le plus utilisé. Lorsque vous êtes sur Google, le serveur enregistre ce que vous tapez afin de vous afficher des publicités selon vos recherches. Le moteur de recherche le plus connu sur la toile pour vous offrir une navigation en toute tranquillité est DuckDuckGo. Pour l'utiliser vous n'avez qu'à taper sur votre moteur actuel : DuckDuckGo et cliquez sur le premier lien. Vous n'avez plus qu'à copier ce lien et vous rendre dans les options pour mettre cette page en page d'accueil.

Refuser les cookies

Sur la plupart de vos navigateurs vous avez une option afin de bloquer tous les cookies. De plus avec cette option les sites vous montrent lorsqu'un cookie est bloqué. Néanmoins certains sites ne peuvent fonctionner que lorsque vos cookies sont activés. Il vous sera alors nécessaire de les accepter pour que le site fonctionne correctement. Cependant vous avez d'autres alternatives : il vous est possible de n'autoriser les cookies que sur certains sites.

Utiliser la navigation privée

La navigation privée est un navigateur web totalement à part : toutes vos informations conservées jusque là ne sont pas utilisées. Cette navigation vous permet donc de naviguer sans que vos données de navigation comme l'historique ou les cookies ne soient conservées. Pour vous mettre en navigation privée vous n'avez qu'à vous rendre dans les paramètres de votre navigateur. Cependant, pour la plupart des navigateurs, il est possible d'activer la navigation en deux clics sans entrer dans les options.
Instructions : http://www.memoclic.com/814-navigateurs/18383-mode-anonyme.html

Forcer des connexions cryptées HTTPS

Pour forcer le cryptage de la plupart des requêtes, le plus simple est d'utiliser l'extension pour Chrome, Firefox et Opera "HTTPS Everywhere" qui rendra autant que possible la communication avec le serveur cryptée.

Bloquer les cookies Flash

Si vous êtes sur Google chrome ou sur Mozilla Firefox, utilisez BetterPrivacy pour vous débarrasser de ces cookies. Sinon vous pouvez bloquer toutes les informations que Flash Player récolte sur vous en faisant un clic droit sur une vidéo, puis ''Paramètres globaux''. Ensuite allez dans l'onglet ''Enregistrement'', cocher ''Empêcher tous les sites [...] sur cet ordinateur''. Dans l'onglet ''Caméra et microphone'' cocher ''Empêcher tous les sites d'utiliser la caméra et le microphone'', puis dans l'onglet dans l'onglet ''Lecture'', cocher ''Empêcher tous les sites [...] en réseau coopérative''.

Désactiver le Javascript

Le Javascript, bien qu'utile à l'interactivité des pages web, peut permettre l'analyse du comportement de l'utilisateur sur ces pages, ainsi que l'exploitation de failles à partir de l'exécution des scripts.
Pour désactiver le javascript, il suffit donc de suivre les indications suivantes :

Firefox: : Tapez dans la barre d'adresse "about:config" puis recherchez le paramètre "javascript.enabled". Changer la valeur de true à false.

Internet Explorer : Outils - Options Internet - Sécurité - Internet - Personnaliser le niveau
et enfin décochez les 3 cases activées de la rubrique script.

Bloquer les publicités/trackers

Il existe un logiciel simple permettant de bloquer les publicités malveillantes, les "pops-ups" (qui sont des pubs qui s'affichent contre votre gré) et les publicités de vidéos : AdBlock. Pour l'installer, rien de plus simple, vous n'avez qu'à taper AdBlock sur votre moteur de recherche, cliquez sur le premier lien et un lien de téléchargement pour votre navigateur apparaîtra. Pour ce qui est des trackers, vous

pouvez utiliser ‘’Ghostery’’, une extension Firefox. Ces trackers, présents sur les pages que vous visitez, enregistrent et analysent vos habitudes de navigation, souvent à des fins commerciales.

Utiliser un proxy

Il existe une application qui permet très simplement la configuration d’un proxy situé aux US, en Angleterre, en Allemagne…etc. Il s'agit d'une extension Firefox qui s'appelle AnonymoX. Celle-ci est gratuite, la connexion est rapide et vous évite de devoir chercher des proxys. Le point fort d’AnonymoX est son côté simple d'utilisation. Pour l’utiliser il faut simplement télécharger l’extension sur : https://addons.mozilla.org/en-US/firefox/addon/anonymox/ et l’installer.
Après avoir redémarré votre navigateur, activez le serveur proxy et choisissez le pays de votre proxy. Vous pouvez maintenant surfer sur votre site préféré et conserver un anonymat relatif avec une IP différente de la vôtre. Il existe d’autres extensions qui permettent de faire la même chose que AnonymoX comme Foxyproxy et Proxy Tool.
Ces extensions permettent de faciliter le changement de proxy, qui peut néanmoins être configuré manuellement dans les paramètres de tous les navigateurs.

Utiliser un VPN

Un VPN rajoute une couche de sécurité entre votre pc et internet. Il crée une liaison cryptée entre vous et une machine distante servant alors d’intermédiaire. En utilisant un VPN, ce n’est alors plus votre pc qui est la cible des attaques mais votre VPN. De plus il vous sécurise lors de connexion à des wifis publics, afin de vous connecter à des sites internet spéciaux et bien d’autres possibilités. Les VPN les plus intéressants sont les VPN payants. En effet, un VPN gratuit ne vous protégera pas totalement étant donné qu’il peut se trouver que le créateur vous vole des informations ou que le serveur du VPN soit instable. Nous pouvons vous conseiller un VPN payant à environ 45€ par an : HideMyAss.

Utiliser le réseau TOR
Allez sur le site Torprojet.org, cliquez sur Download Tor, puis cliquez sur Download Tor Browser. Il s’agit de la technique la plus simple pour utiliser le protocole Tor. Tor Browser est en fait une version modifiée de Firefox qui intègre nativement le protocole Tor.
Installez le navigateur et lancez le. Une fenêtre apparaît. Cliquez sur “se connecter” directement si vous souhaitez commencer à surfer en mode anonyme, mais il est obligatoire de passer par “Configurer” si votre FAI censure certains protocoles, filtre une partie du trafic ou vous fait passer par un proxy. Dans ce cas, il faudra passer par une passerelle qui va masquer votre point d’entrée dans le réseau. Pour activer ce “protocole obfuscation” (=Stratégie de protection de la vie privée sur internet qui consiste à publier des informations fausses ou imprécises de manière à dissimuler les informations pertinentes) répondez YES à la troisième question et utilisez le obfs3 comme recommandé.
Enfin cliquez sur “Connect”. Si vous voyez “Félicitation ! Ce navigateur est configuré pour utiliser Tor”, c’est que vous êtes libre de surfer où bon vous semble sur internet.
Le moteur de recherche par défaut du navigateur est lxquick et les modules HTTPS Everywhere et NoScript sont activés. Le premier permet de forcer l’utilisation du protocole HTTPS par le serveur tandis que le second désactive tous les scripts sur le navigateur.

- **Glossaire**

Cookie : Court fichier stocké sur l'ordinateur de l'utilisateur permettant de garder une information en mémoire pour une prochaine visite. Exemple : le score d'un jeu sur navigateur, les identifiants de connexion, l'identité, les préférences…

Cookie Flash (*LSO : Local Shared Object*) : Comme les cookies, ils permettent de garder des informations en mémoire pour une prochaine visite. Ils sont cependant plus lourds, moins visibles, et reposent sur Adobe Flash.

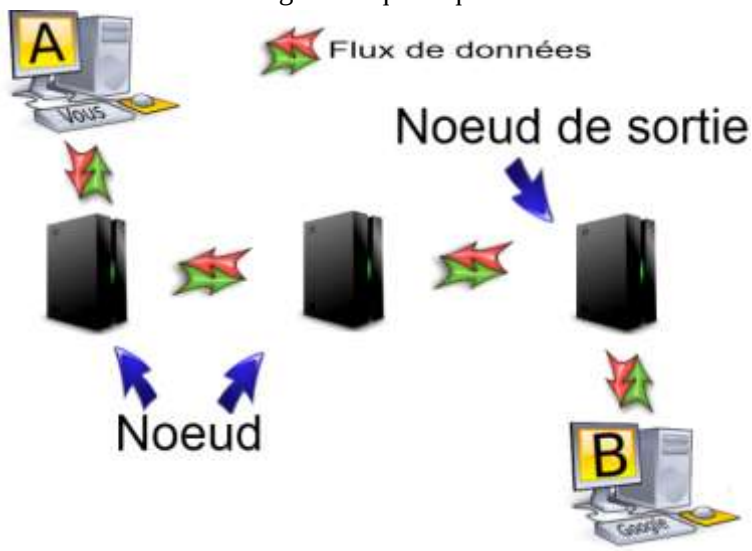
HTTPS (*HyperText Transfert Protocol Secure*) : Protocole servant principalement à la communication cryptée entre le client et le serveur web (cryptage SSL).

Javascript : Langage de programmation de scripts le plus utilisé sur les pages Web. Il permet de rendre ces pages dynamiques et interactives, tant visuellement que dans leur contenu.

Proxy : Un proxy est un serveur jouant le rôle d'intermédiaire entre le client et Internet : toutes les communications vers l'extérieur passent par celui-ci. Il permet ainsi de cacher l'adresse IP du client ainsi que sa position géographique. Les données entre le client et le proxy sont néanmoins transmises en clair (=sans cryptage).

Tracker : Élément d'une page web permettant de récolter des informations sur ses visiteurs à des fins statistiques. Elles sont cependant en grande partie fournies par des régies publicitaires afin de mieux cibler l'affichage des publicités.

TOR (*The Onion Router*) : TOR est un réseau de clients connectés. Il sert d'intermédiaire entre un client membre du réseau et Internet, en faisant passer la requête à travers un nombre aléatoire de "noeuds", c'est-à-dire de clients du réseau. Il rend ainsi le suivi des utilisateurs très difficile car la machine du réseau accédant à Internet change à chaque requête.



VPN (*Virtual Private Network*) : Un VPN, ou réseau privé virtuel, est un système créant un lien entre deux machines via un tunnel sécurisé. Ce tunnel peut alors permettre à une des machines d'accéder à Internet depuis l'autre machine, qui sert d'intermédiaire. Comme le proxy, ce système permet de masquer l'IP et la géolocalisation du client.