SNT05.4

COOKIES, SÉCURITÉ ET CONFIDENTIALITÉ

manuel utilisé et mentionné dans cette fiche →

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.”

Prétendre que vous vous fichez du droit à la vie privée parce que vous n’avez rien à cacher n’est pas différent que de dire que vous vous fichez de la liberté d’expression car vous n’avez rien à dire.

Edward Snowden[1]

COOKIES

Un cookie (appelé aussi « cookie HTTP ») est une suite d’informations (texte), généralement de petite taille et identifié par un nom, qui peut être transmis à votre navigateur par un site web sur lequel vous vous connectez. Ce fichier est stocké dans un dossier du navigateur, sur le disque dur de l’ordinateur.

Le contenu d’un cookie est déterminé par le site web qui l’a créé, et varie d’un site à un autre.

De manière générale, les cookies contiennent des caractères alphanumériques aléatoires.

Toutes les informations personnelles qu’ils peuvent contenir sont le résultat de vos visites, de votre comportement sur le site et de votre propre saisie sur le formulaire du site.

Très souvent (mais pas toujours), lorsqu’un cookie stocke des informations personnelles, elles sont chiffrées : le seul ordinateur qui peut lire et décoder les informations est le serveur qui a créé le cookie en premier lieu.

Dans l’ensemble, il existe deux grands types de cookies :

– **Cookies de session**

Ils sont temporaires et expirent dès que vous fermez le navigateur. Ce type de cookie est surtout utilisé par les boutiques en ligne qui gardent en mémoire les articles que vous avez placés dans le panier pendant une même session d’achat.

De nos jours, les applications comme les paniers d’achat enregistrent plutôt la liste des articles dans une base de données sur un serveur, plutôt que de les enregistrer dans le cookie lui-même : le serveur web envoie un cookie contenant un identifiant de session unique ; le navigateur web renvoie alors cet identifiant de session à chaque requête suivante et les articles du panier sont enregistrés et associés avec ce même identifiant unique de session.

– **Cookies permanents (ou persistants)**

Ils restent dans un des sous-dossiers de votre navigateur jusqu’à ce que vous les supprimiez manuellement ou que votre navigateur les supprime selon la durée précisée dans le cookie. Bien que

1 Edward Snowden (né en 1983) est un lanceur d’alerte américain. Informaticien, ancien employé de la Central Intelligence Agency (CIA) et de la National Security Agency (NSA), il a révélé le 5 juin 2013 les détails de plusieurs programmes de surveillance de masse américains et britanniques. À la suite de ses révélations, il est inculpé le 22 juin par le gouvernement américain sous les chefs d’accusation d’espionnage, vol et utilisation illégale de biens gouvernementaux. Il risque 30 ans de prison !
S’exilant à Hong Kong puis à Moscou, Edward Snowden obtient le 31 juillet 2013 l’asile temporaire en Russie.
Le 1er août 2014, il obtient un droit de résidence pour trois ans en Russie.
Le 18 janvier 2017, la Russie prolonge son droit d’asile de trois ans (jusqu’en 2020).
Le 16 septembre 2019, Snowden a réitéré son souhait d’être accueilli par la France. Il assure avoir demandé en vain l’asile à Paris dès 2013, sous la présidence de François Hollande. Mais, le 19 septembre 2019, jour de la sortie en France de son autobiographie *Mémoires vives*, sa demande est rejetée.

la loi exige que ces cookies soient supprimés après maximum 12 mois, certains cookies peuvent rester sur votre disque pour toujours. : ils peuvent retenir des données telles que vos informations de connexion, vos coordonnées et vos numéros de compte pour que vous n'ayez pas à les entrer à chaque fois que vous utilisez un site.

On peut aussi classer les cookies d'une autre façon :

– **Cookies internes (ou « cookies HTTP » ou « first party cookies »)**

Ces cookies sont créés par le site auquel vous avez accédé : ils servent généralement à permettre au site de se souvenir de vos données et de vos préférences.

– **Cookies tiers (ou « cookies tierce partie » ou « third party cookies »)**

Ils sont créés par un autre site que celui auquel vous avez accédé.

Les images et autres objets contenus dans une page web peuvent résider dans des serveurs différents de celui hébergeant la page.

Par exemple, un site peut avoir un bouton « J'aime » de Facebook sur ses pages : ce bouton activera un cookie pouvant être lu par Facebook. Le but des cookies tiers est souvent de recueillir certaines informations destinées à se renseigner sur votre comportement et à vous pister à des fins de marketing ciblé, etc.

Les données stockées dans les cookies sont très intéressantes pour les exploitants de sites Web, car **ils peuvent en tirer des statistiques et des conclusions sur le comportement de navigation des visiteurs**.
Les cookies tiers sont particulièrement efficaces pour cela : ils sont généralement mis en place par des tiers, sans être remarqués, et **espionnent le comportement de navigation des utilisateurs**, généralement sur une longue période de temps et sur différents serveurs. Par exemple, si vous visitez fréquemment des sites web consacrés à la santé, il est probable que vous verrez bientôt plus de publicités pour des médicaments, même sur des sites qui n'ont rien à voir avec le sujet. Un autre utilisateur est susceptible de voir de la publicité différente sur le même site parce que son profil d'utilisateur révèle un intérêt pour un domaine différent.

ATTENTION

Vous devez être particulièrement prudent lorsque vous naviguez sur un ordinateur public ou chez quelqu'un : les cookies stockés localement sont en théorie accessibles à tout utilisateur ultérieur de l'ordinateur, de sorte que vos données personnelles peuvent se retrouver dans de mauvaises mains.

À RETENIR

• Chaque cookie ne peut contenir que du texte, et ne peut donc pas être exécuté comme un programme ni contenir de "virus".

• Chaque site à ses propres cookies et ne peut donc pas lire les cookies d'un autre site.

• Les cookies ont habituellement une date d'expiration, qui oscille entre quelques secondes et plusieurs dizaines d'années. Mais ils peuvent être supprimés librement et à tout moment via le navigateur sans attendre une quelconque date.

Pour info : • chaque cookie a une taille maximum de 4 ko environ (l'équivalent de quelques phrases) ;
• environ 50 cookies max. par domaine (cela change en fonction des navigateurs).

POURQUOI COOKIE ?

Cookie = « biscuit » en anglais.

Un *fortune cookie* est un biscuit croquant, accompagné d'un message surprise comme un proverbe, servi dans les restaurants chinois du monde entier.

IL N'Y A PAS QUE LES COOKIES

D'autres méthodes sont utilisées pour pister les internautes. En voici quelques-uns :

– **le pixel espion (ou « pixel invisible » ou « balise web »)**

Cette technique consiste à appeler une image invisible de l'internaute (taille = 0 ou 1 pixel), hébergée sur un serveur tiers. Lors de cet appel, des informations sont transmises en paramètre de la requête HTTP/GET correspondante.

Exemples de code HTML incluant un pixel invisible :

```
<img src="http://jetepiste.com?&img=d690a7357b.png » style="visibility : hidden">
```

```
<img src="http://jetepiste.com?&img=d690a7357b.png » style="display : none">
```

```
<img src="http://jetepiste.com?pixel.png?pid=AZY8yBmmTLHS » width="0 » height="0">
```

Dans ces exemples, en ouvrant la page web ou le courrier électronique qui contiendrait un de ces codes, le navigateur de l'internaute effectue une requête de type GET vers `jetepiste.com`. Il transmet alors un paramètre : un nom d'image (`d690a7357b.png`) ou un contenu de variable (`pid=AZY8yBmmTLHS`). Ce paramètre unique, permet alors de reconnaître l'internaute et donc de savoir qu'il a consulté telle partie d'une page internet ou qu'il a ouvert tel e-mail publicitaire.
En réponse, le serveur web peut déposer un ou plusieurs cookies via l'en-tête « SET-COOKIE » du protocole HTTP. Dès lors, à chaque fois que l'internaute se rendra sur un site web contenant un code redirigeant vers le domaine `jetepiste.com`, il sera pisté.
Ces données peuvent alors êtres vendues à (ou utilisées par) des sociétés publicitaires.

– **les *local shared objects* (LSO ou « cookies flash »)**

Données enregistrées sur l'ordinateur de l'internaute, lors de l'exécution d'applicatifs Flash (Adobe Flash Player et Macromedia Flash MX Player).
Par défaut, l'applicatif Flash peut écrire sur le terminal de l'utilisateur sans avoir requis préalablement le consentement de l'utilisateur.

– **le *local storage* (« stockage web local »)**

HTML (version 5) apporte une nouveauté par rapport à ses prédécesseurs : la possibilité de stocker des données dans le navigateur sans utiliser de cookies. Cette technique permet de sauvegarder des volumes de données plus importants qu'avec les cookies (entre 5 Mo et 10 Mo max. contre 4 ko max. pour les cookies).

Il existe deux types de stockage web local : le `localStorage` et le `sessionStorage`, équivalent respectivement aux cookies persistants et aux cookies de session.
Cette solution est couramment utilisée par les développeurs voulant se prémunir du blocage des cookies, car elle n'est elle-même pas facilement bloquée.

Globalement, le contenu utilisé pour le pistage peut comprendre des publicités, des champs de connexion, des formulaires, des paiements, des commentaires, des vidéos et des photos, des boutons…

SÉCURITÉ ET CONFIDENTIALITÉ : PARAMÉTRER SON NAVIGATEUR

L'élément dont il est le plus simple de se passer sont les cookies tiers : ces derniers ne sont que très rarement utilisés à des fins légitimes et il est assez rare qu'un site ne fonctionne pas parce qu'ils sont entièrement désactivés.

C'est donc presque la première chose à faire lorsque vous configurez un navigateur. En cas de souci, il est de toute façon possible, dans la plupart des cas, de gérer des exceptions domaine par domaine pour s'assurer d'un retour à la normale.

Vous pouvez également bloquer entièrement les cookies, mais cela posera souvent des problèmes pratiques, notamment parce qu'ils permettent de gérer de nombreux dispositifs techniques comme la connexion à un site, vos préférences, etc. Si besoin, optez plutôt pour une approche au cas par cas.

Regardons comment faire cela sur le navigateur Firefox :

La navigation privée

Faire « Fichier → Nouvelle fenêtre de navigation privée » ou « Ctrl+Maj+P ». La navigation privée permet de masquer votre activité en ligne des autres personnes qui utilisent Firefox sur votre ordinateur.

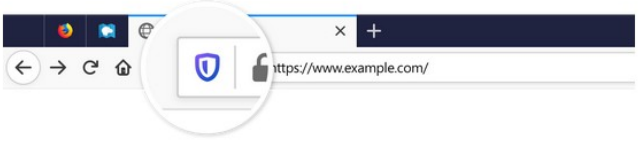
ATTENTION AUX IDÉES REÇUES

La navigation privée vous rend anonyme sur Internet ? **FAUX**

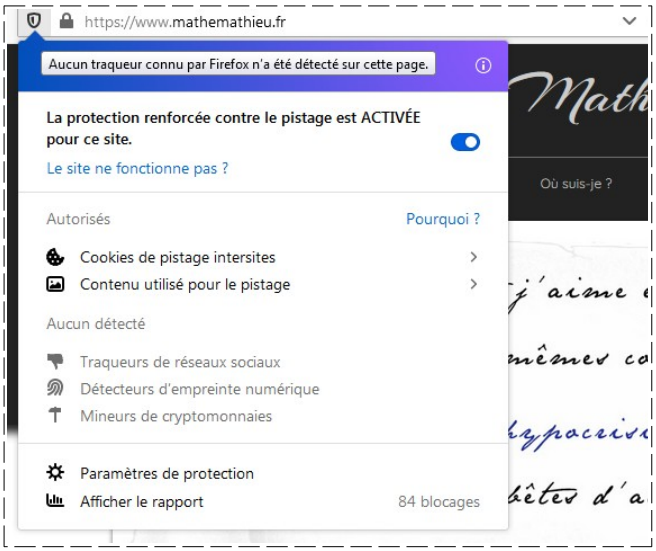
La navigation privée supprime toute trace de vos activités sur Internet de votre ordinateur ? **FAUX**
(un fichier téléchargé, un site mis en favori, etc. tout cela n'est pas supprimé)

La navigation privée vous protège des enregistreurs de frappe et des logiciels espions ? **FAUX**

Protection renforcée contre le pistage



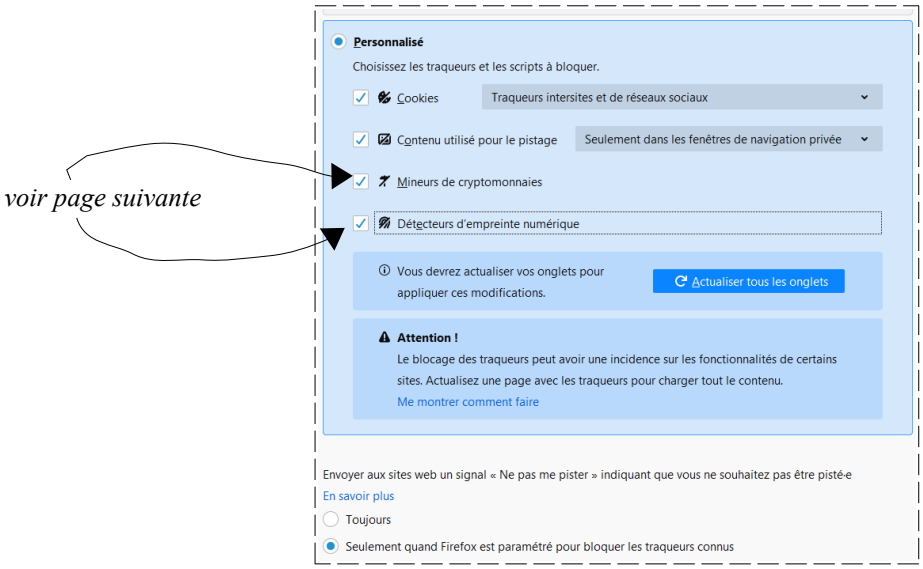
- – **Violet :** Firefox a bloqué des traqueurs et des scripts malveillants sur un site. Ouvrez le bouclier pour voir ce qui a été bloqué.
- – **Gris :** aucun traqueur ou script malveillant connu n'a été détecté sur un site.
- – **Gris et barré :** la protection renforcée contre le pistage est désactivée pour un site. Ouvrez le bouclier et basculez le commutateur pour l'activer de nouveau.



Si un site semble dysfonctionner, essayez de désactiver la protection renforcée contre le pistage. Les traqueurs ne sont autorisés à se charger que dans ce site. La protection renforcée contre le pistage va continuer de bloquer les traqueurs dans les autres sites.

Pour savoir ce qui a été bloqué sur tous les sites au cours de la dernière semaine, cliquez sur le bouton de menu (trois barres horizontales, en haut à droite) et sélectionnez *Protections de la vie privée* (autre solution : saisir « `about : protections` » dans la barre d'adresse).

En cliquant ici (ou faire « Outils → Options → Vie privée et sécurité ») :



voir page suivante

Qu'est-ce que les « mineurs de cryptomonnaies » ?

Ce sont un type de logiciel malveillant (malware) qui utilise la puissance informatique de votre système pour miner* de la cryptomonnaie. Les scripts de minage déchargent votre batterie, ralentissent votre ordinateur et peuvent augmenter votre facture d'énergie.

* Générer des cryptomonnaies nécessite généralement de résoudre un problème cryptologique complexe : miner, c'est tenter de résoudre ce problème. Il s'agit d'un processus gourmand en ressources qui consomme donc beaucoup d'énergie et de puissance informatique. Pour éviter des coûts, les mineurs de cryptomonnaies déploient ces scripts sur les ordinateurs d'autres personnes sans leur consentement pour capter énergie et puissance de calcul à leur profit.

Qu'est-ce que les « détecteurs d'empreinte numérique » ? (appelé aussi le *fingerprinting*)

Les détecteurs d'empreinte numérique recueillent les paramètres* de votre navigateur ou de votre ordinateur pour dresser votre profil.

* les extensions que vous utilisez, le système d'exploitation et le modèle de votre appareil, la résolution de votre écran et la langue, des informations sur votre connexion réseau, les polices d'écriture installées sur votre ordinateur, etc.

En utilisant cette empreinte numérique, ils peuvent créer un profil unique de vous pour vous pister sur divers sites web.

Pour voir de nombreux paramètres qui forment votre *empreinte numérique* sur l'ordinateur sur lequel vous lisez cette page, allez visiter ce site tout à fait sérieux : https://amiunique.org/fp
Contrairement à d'autres sites, celui-ci est open source. Mais comme beaucoup d'autres sites analogues, il se propose de mesurer le niveau de protection de votre navigateur face au suivi publicitaire et évalue un score "d'unicité" : la conclusion "unique" de votre navigateur par ces sites Web peut être inexacte et trompeuse. Voici pourquoi :

– les empreintes digitales de votre navigateur sont comparées à une base de données géante de navigateurs anciens et obsolètes, dont beaucoup ne sont plus utilisés. Lorsque vous testez les empreintes digitales de votre navigateur avec un navigateur mis à jour, il est possible qu'elle apparaisse comme extrêmement rare et unique, même si la majorité des utilisateurs utilisent la même version mise à jour. À l'inverse, l'exécution du test avec un navigateur ancien et obsolète peut donner un très bon résultat (non unique) alors qu'en réalité, très peu de personnes utilisent aujourd'hui l'ancien navigateur.

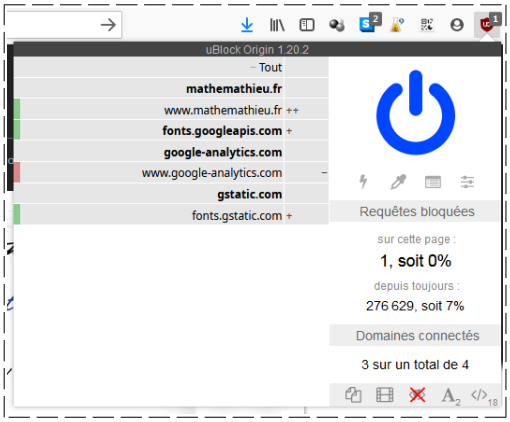
– au moins sur les ordinateurs de bureau, la plupart des gens ajustent régulièrement la taille de l'écran de leur navigateur. Chaque valeur de taille d'écran mineure sera mesurée en tant que facteur d'unicité, ce qui peut être trompeur.

– ces sites ne tiennent pas compte des empreintes digitales aléatoires qui peuvent être changées régulièrement via des extensions de navigateur. Cette méthode peut constituer un moyen efficace d'empêcher les empreintes digitales dans le monde réel, mais elle ne peut pas être testée ou quantifiée via ces sites.[2]

2 Source : https://pypo.eu/solutions/navigation-securisee/tester-et-attenuer-empreinte-de-votre-navigateur/

Des modules/extensions à rajouter

Vous pouvez utiliser, par exemple, le module ***uBlock Origin***, qui bloque les publicités et les pisteurs.



Le gros bouton « power » permet de désactiver/activer en permanence *uBlock* pour le site web en cours de consultation.

Autre module indispensable : ***HTTPS Everywhere***.
Certains sites ne chiffrent pas les données (potentiellement personnelles ou sensibles) contenues dans des cookies qu'ils déposent sur le terminal de l'internaute.
Il en résulte que, sur les pages accessibles en HTTP, les cookies contenant un certain nombre de données personnelles sont transmis en clair.
L'extension *HTTPS Everywhere* protège vos communications en activant automatiquement le chiffrement HTTPS sur les sites le prenant en charge, même lorsque vous saisissez une URL ou cliquez sur un lien sans préfixe « https : ».

Pour terminer, si vous pensez que les vols/violations de données sont rares, vous vous trompez c'est même le contraire ! Choisissez un des deux articles suivants et notez ici deux vols/violations qui vous semblent incroyables :

- article 1 : Les 10 plus grandes violations de données en 2018
- article 2 : 2019 a été une « année record » en termes de violations de données

Vol/violation n°1 :

Vol/violation n°2 :

COMPLÉMENTS

Si vous voulez voir à quel point un cookie est important, regardez cette vidéo (≈ 12 min) de Micode sur une technique de phishing élaboré (ici sur Facebook avec double authentification, utilisation d'un cookie pour y arriver).
À la fin, deux conseils sont donnés pour éviter le phishing : utilisation d'un gestionnaire de mots de passe (personnellement j'utilise KeePass) ou utilisation d'une clé physique U2F (lien1 et lien2).