

[Fiche 04] L'historique de navigation et les cookies

Présentation

[Edge](#), [Google Chrome](#), [Mozilla Firefox](#) (évoqués dans la [fiche 1](#)) stockent un grand nombre d'informations durant les navigations. Il s'agit de traces concernant les recherches et les pages des sites visités.

Ces traces comportent :

- un historique des navigations avec des éléments d'identification des pages (adresse HTTP, date de visite...),
- une mémorisation des éléments indiqués par l'utilisateur (données de formulaire, données d'identification à des sites Internets et mots de passe...),
- des données conservées visant à faciliter les navigations ultérieures (cache, préférences de sites, cookies).

L'ensemble de ces informations est appelé "l'historique de navigation". Celui-ci permet à l'internaute de retrouver facilement les sites visités et de ne pas avoir à refournir toujours les mêmes informations. La mémorisation de ces saisies s'effectue par défaut et souvent de façon automatique. Toutes ces informations sont conservées sur l'ordinateur de l'utilisateur. Parmi ces informations sont stockés des petits fichiers textes appelés "cookies". Ces suites d'informations sont créées et enregistrées à la demande du site visité. Ces cookies peuvent apporter des facilités pour se connecter ultérieurement, pour conserver des paramètres ou pour utiliser un site en général. Ils sont souvent nécessaires pour réaliser des achats en ligne. Il ne s'agit pas de fichiers exécutables et ce ne sont pas des virus, mais étant interrogeables, ils offrent des possibilités de traçage des activités de l'internaute. Par exemple, même sans être "cliqués", les boutons de partage des réseaux sociaux, présents sur de nombreuses pages, permettent à Facebook, Google et Twitter de tracer les visites. Pour se préserver de cette intrusion : [voir la fiche 5](#)

Limiter les traces locales de ses communications sur Internet

Afin de réduire ces traces, les principaux navigateurs Internet proposent des outils de navigation "privée". La navigation privée permet, théoriquement, d'utiliser Internet en minimisant les traces sur son propre ordinateur : lorsque l'outil est activé, il n'y a pas d'enregistrement d'historique de navigation, de données de formulaires, des téléchargements effectués, ni de conservation de cookies. Les données sont utilisées dans l'immédiat, mais sont supprimées dès la fin de l'opération ou de l'activité de l'internaute.

À titre d'exemple, il est possible de lancer une fenêtre de navigation privée sur Firefox en appuyant sur : "Ctrl + Maj + P" (ou Pomme + Maj + P sur Mac) ou en cliquant "Nouvelle fenêtre de navigation privée" dans les options.

Il faut d'ailleurs noter que [depuis quelque temps](#), la navigation privée de Firefox offre aussi une protection contre le traçage ([voir fiche 5](#)) !

Il est aussi possible de demander à Firefox de ne jamais conserver d'informations :

dans l'onglet "Vie privée" des "Options" (ou "Préférences"), choisir le paramètre "ne jamais conserver l'historique".

Sans utiliser la navigation privée, on peut également supprimer tout ou partie de l'historique de navigation régulièrement.

toujours dans l'onglet "Vie privée", cliquer sur "Effacer votre historique récent", ou, à partir du Menu, onglet "Historique", puis "Supprimer l'historique récent".

Choisir les éléments que l'on souhaite supprimer ou conserver et définir la période de suppression.

On peut ainsi supprimer toutes les traces temporaires et ne conserver que les favoris et autres mots de passe enregistrés. L'utilisation de la navigation privée ou la suppression manuelle de l'historique sont des fonctions importantes en particulier si l'ordinateur est partagé. C'est par exemple le cas pour l'utilisation d'un ordinateur public. Il s'agit là de protéger sa vie privée face aux personnes ayant accès au même ordinateur qui peuvent être des proches ou non.

Les limites de la gestion locale de ses traces

L'utilisation de la navigation privée ne protégera toutefois pas de nombreuses possibilités de surveillance des communications ou des données de connexion par :

- des sites Web consultés,
- des employeurs ou gestionnaires locaux de l'accès réseau (selon les paramètres choisis),
- les Fournisseurs d'Accès Internet,
- des mouchards malveillants, virus ou intrusions sur la machine,
- d'une interception en direct de la communication.

Même s'il s'agit d'une protection limitée, il est important de connaître et maîtriser la gestion de ses propres traces. Cela permettra d'éviter que des proches ou un tiers indésirable ne prennent facilement connaissance d'informations jugées personnelles. Cela n'empêchera toutefois pas d'être tracé et profilé par de grandes entreprises en ligne, ni de limiter les possibilités de surveillance des États. D'autres solutions doivent être mises en œuvre, qui elles aussi ont leurs limites. Pour cela, direction [les autres fiches !](#)

Pour aller plus loin :

La CNIL dispose d'une documentation assez complète sur les enjeux des cookies au regard de la vie privée. Ces informations sont regroupées dans un dossier [sur les cookies et autres traceurs](#). Elle dispense ainsi des conseils [côté utilisateur](#), mais aussi sur les [obligations des responsables de site à cet égard](#). Elle a également mis au point un outil, [Cookieviz](#), malheureusement uniquement disponible sur Windows, qui permet de visualiser la création et le fonctionnement des cookies sur votre ordinateur ([il existe une vidéo de présentation](#)).

Fiche 4 [publiée le 2 avril 2015, dernière mise à jour avril 2018]