

Le saviez-vous?

Lorsque vous chargez une page depuis le web, vous pensez sans doute ne charger que son contenu depuis le site défini dans l'URL. Eh bien non ! La grande majorité des pages web contactent d'autres sites, en général via des routines écrites en JavaScript. Ces sites collectent le plus souvent des informations sur vos habitudes et sur les sites que vous fréquentez, pour cibler la publicité que vous verrez apparaître, par exemple lorsque vous faites une recherche sur Google ou Bing.

Il est néanmoins possible d'éviter ces retours d'information (au moins partiellement) en utilisant, par exemple, le plug-in « Ghostery » dans votre navigateur. Une fois installé, ce plug-in vous montre les sites appelés depuis la page que vous venez de charger. Exemple :

The screenshot shows the CERN Directory website. The browser address bar displays 'directory.web.cern.ch/directory/'. The page features a search bar with the text 'Phonebook search' and a 'Search' button. Below the search bar, there are several sections: 'Departments, groups and units', 'Experiments and projects', and 'Applications'. A red arrow points to a 'Google Analytics' button in the bottom right corner, with the text 'Ce site est appelé depuis la page d'entrée du CERN' next to it.

Lorsqu'on invoque la page d'entrée du CERN, celle-ci envoie des informations au site « Google Analytics ». Si on examine le code source de la page web, on retrouve en effet cet appel, via un script généré au sein de la page :

```
<script type="text/javascript">
//Google Analytics
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8058079-24']);
_gaq.push(['_trackPageview']);
(function() {
  var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async =
true;
  ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') +
'.google-analytics.com/ga.js';
  var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);
})();
</script>
```

« Google Analytics » est un des sites les plus fréquemment invoqués, car il permet au propriétaire de la page appelée d'obtenir des statistiques sur l'utilisation de cette page. Mais aussi sur les habitudes des visiteurs d'un site, d'où vous vous connectez, etc. « Yahoo Analytics » ou « Adobe Test & Target » sont de la même veine. D'autres sites appelés « en catimini » sont bien moins recommandables. Prenez l'exemple du site Swisscom TV :

The screenshot shows the Swisscom TV website interface. On the left, a sidebar titled "Détecté 9 mouchards" (Detected 9 trackers) lists various tracking tools: Adition, Adobe-Test & Target, Facebook-Connect, Google AdWords Conversion, Google+ Platform, and LivePerson. Below this list are buttons for "Suspendre le blocage" (Suspend blocking) and "Autoriser le site web" (Allow website). A red arrow points from the text "Détails de mouchards" (Tracker details) to the "Autoriser le site web" button.

The main content area is titled "Overview of Swisscom TV offerings" and features three service packages: Swisscom TV 2.0 plus, Swisscom TV 2.0 basic, and Swisscom TV 2.0 light. Each package includes details on channel counts, replay functions, and recording capabilities. A red arrow points from the text "Ces sites sont appelés depuis la page d'entrée de Swisscom TV" (These sites are called from the Swisscom TV landing page) to a purple box listing the tracked sites: Adition, Adobe-Test & Target, Facebook-Connect, Google AdWords Conversion, Google+ Platform, LivePerson, Omniture (Adobe-Analytics), Tealium, and Twitter-Bultron.

Surprise ! 9 sites sont appelés depuis cette page, dont des sites de réseaux sociaux comme « Facebook » ou des sites publicitaires comme « Adition » ou « Google AdWords Conversion ». Là on peut commencer à se poser des questions...

Ghostery permet donc d'identifier les « mouchards », mais aussi de les bloquer. Ce plug-in est disponible gratuitement pour la majorité des navigateurs depuis le site de son développeur : <https://www.ghostery.com>. Sur le lien <https://www.ghostery.com/fr/how-we-make-money> vous trouverez les explications comment ils gagnent de l'argent et ce qu'ils font et ne font pas lorsque vous activez leur suivi.

Tout de suite après l'installation du plug-in Ghostery, le navigateur affiche une fenêtre de configuration. On peut alors choisir de bloquer l'accès aux sites « mouchards » globalement, par catégorie ou individuellement. Ghostery permet aussi de voir les détails des « mouchards » en cliquant sur la petite icône de fantôme en haut à gauche de la fenêtre. En cliquant sur la roue dentée de la fenêtre des détails, on accède aussi aux réglages des paramètres de Ghostery. On peut alors visualiser la liste des sites bloqués, en autoriser certains si on le souhaite, etc.

Sur le site <http://www.google.com/analytics/why/> vous trouverez (en anglais) les avantages que propose Google Analytics à ses clients. Par exemple, que vous pouvez suivre ce que fait un visiteur après avoir cliqué sur une annonce. Assez édifiant par rapport au respect de la vie privée...

Notez enfin que le site du Micro Club, bien qu'hébergé au CERN, ne contacte pas d'autres sites. Possible, puisque c'est dans le code de la page chargée que se trouvent les scripts et que nous n'en mettons pas.