

INTRODUCTION TO COOKIES

COMMUNICATION & COLLABORATION > 2.6 MANAGING DIGITAL IDENTITY

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
All, Low literacy citizens, School drop outs, Students (secondary school)	Adults, Elderly citizens, Teenagers	Level 2	Activity sheet	Creative Commons (BY-SA)	English, French

This activity will develop participants' understanding of cookies and targeted advertising. It will also draw attention to ways in which websites operate in order to allow advertisers to track our activity.

General Objective Knowledge acquisition

Preparation time for facilitator less than 1 hour

Competence area 1 - Information and data literacy

Time needed to complete activity (for learner) 0 - 1 hour

Name of author Nothing 2hide

Support material needed for training Computers - Video projector (optional)

Resource originally created in French

WORKSHOP DIRECTIONS

1 Introduction

This workshop has two objectives:

- Develop awareness in participants that in just by using the internet, they become the targets of ad tracking.
- Be a guide to controlling and limiting ad tracking.

Facilitation tips: It is important to download Mozilla Firefox prior to the beginning of the workshop, as the activities are designed based on this search engine in particular. You should also, depending on the amount of time at your disposal, download and install a complementary module, and we advise you to do this beforehand. The instructions for installations are found in part 4 of this sheet. You can finish the activity with a [walking debate](#) on the subjects of personal data and privacy.

2 What is a cookie?

A cookie is a small text file that websites are able to leave on your computer via your browser. Historically, they were created during the 1990s to improve the experience of internet users and to address issues on the earliest retail sites which, in the event of any connection interruption, would empty their customers' baskets. The idea was to deposit a file on the user's computer which was sent and read by the retail site at the moment of reconnection so that it recognises the visitor. This could for example allow a site to remember you and show you the most recent articles you read. With the evolution of retail sites, the use of cookies has advanced and they are now used generally by advertisers to target and study behaviours of potential online buyers. For more information, we advise you to refer to the activity sheet '[Personal data](#)'.

3 Using Firefox

Ask participants to open Firefox and go to the following websites:

1. <https://www.amazon.com/>
2. <https://www.theguardian.com/>
3. <https://www.decathlon.com/>
4. <https://www.digitaltrends.com>
5. <https://www.behance.net/>

Recommend they take 10 minutes in total so they can have a look at each website.

4 Finding your cookies

Now, show participants that in fact, without their knowledge, they visited a lot more than five sites. This is in the sense that their information was communicated to other websites with no apparent connection to those visited. Let's take a look behind the scenes. Install the extension LightBeam:

<https://addons.mozilla.org/fr/firefox/addon/lightbeam-3-0/>



Firefox Lightbeam by Mozilla

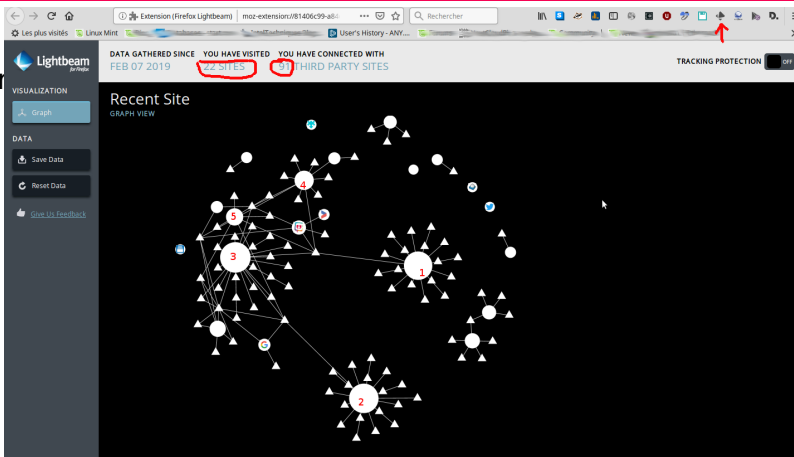
Lightbeam is a Firefox add-on that enables you to see the first and third party sites you interact with on the Web. Using interactive visualizations, Lightbeam shows you the relationships between these third parties and the sites you visit.

+ Add to Firefox

How to install: Click 'Add to Firefox' and give the permission requested by Firefox. A new icon (LightBeam) will appear to the right of the search bar.

How does this work? The extension will simply analyse the cookies – the vestiges of your internet navigation – kept in Firefox's memory. Clicking on the icon will open a tab and the analysis will begin. Bubbles will appear: the large ones represent the sites you visited and everything surrounding them represent the sites with which the visited sites communicate and exchange user information. After quickly explaining how LightBeam works, ask the group to open the sites from the previous list – a different tab for each – and now to refer back to the LightBeam tab. They will see the cookies working in real time! It frequently happens even that without any activity from the user – simply opening the pages and leaving them – new bubbles appear. In the screenshot below, although I have only visited 5 sites, you can see that my browser visited or exchanged information with 113 sites without informing me or

asking per



ual sites so they can develop their

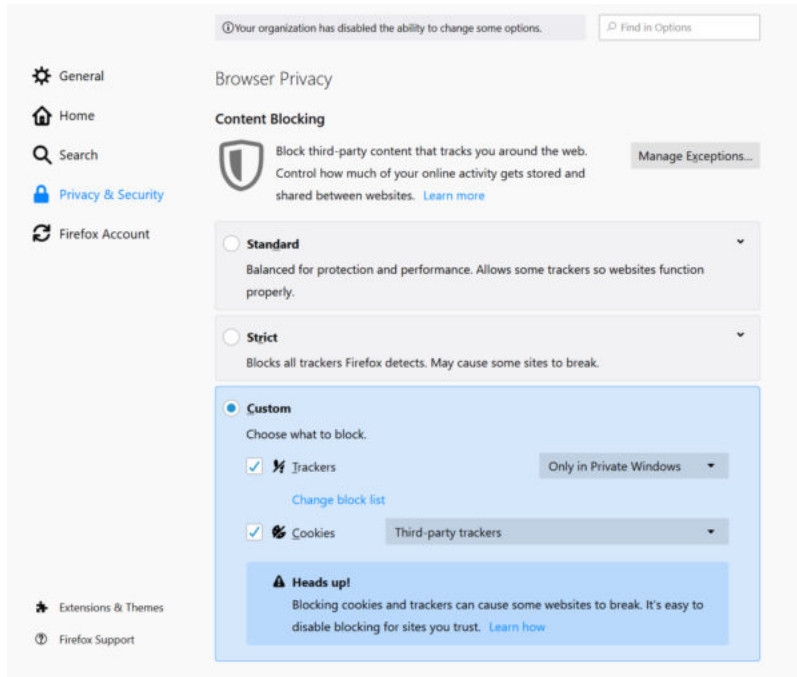
thoughts.

5 Protecting ourselves from trackers

There are many easily installable cookie blockers available. For example :

- PrivacyBadger: <https://addons.mozilla.org/en-US/firefox/addon/privacy-badger17/>
- uBlock: <https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/>
- Disconnect: <https://addons.mozilla.org/en-US/firefox/addon/disconnect/>

It is also possible to change your browser settings to block cookies. On Firefox for example, in browser preferences, click on 'Privacy & Security' and in the section 'Content Blocking' choose **Strict**.



Once one you have installed one of the extensions listed above or once you have changed your browser settings, repeat the previous exercise and visit five new sites (or the same, but first you would need to clear your LightBeam data using the 'reset data' button). Now, many fewer signs of trackers should appear. It is also possible to do a test by messing with the 'Tracking Protection ON/OFF' button which will show very clearly cookies you receive from sites depending on whether you have protection activated or not.