# Browser Extensions to make you safer: HTTPS Everywhere and Privacy Badger: beginning

Browsing the web can be tricky: avoiding unsecured HTTP sites and avoiding the data collection of trackers can be a challenge. That's where two EFF browser extensions come in: one to offer additional security, and one to offer additional privacy.

The HTTPS Everywhere browser extension defaults to secure connections of HTTPS when browsing websites. And the Privacy Badger extension helps you avoid spying ads and third-party trackers trying to collect data on your habits as you move site to site. In this lesson, we will share some ways for learners to protect their information as they browse the web.

## Recommended Reading

- Different Types of Encryption
- Web Browsing Security
- Five EFF Tools to Help You Protect Yourself Online
- Privacy Badger website
- HTTPS Everywhere website
- Panopticlick website
- Encrypting the Web
- Moxie Marlinspike's SSLstrip attack information

## Gotchas and Problems You Might Hit

You might hit some misconceptions about these two tools.

### Privacy Badger and HTTPS Everywhere Aren't 100% Solutions

It's worth making clear what these browser extensions are meant to address—and what they aren't.

**The threat model for Privacy Badger:** Privacy Badger stops companies from compiling information on your browsing patterns — it only provides marginal protection from attackers who are trying to target you directly, like criminals, stalkers, or governments.

**The threat model for HTTPS Everywhere:** HTTPS Everywhere helps increase the level of **encryption** you use everyday, which does increase your protection against mass surveillance or someone spying on your web traffic, but it doesn't encrypt *all* of your communications.

Think of them both as vitamins. They give most people improved protection on a daily basis, but if you're suffering from a particularly serious attacker, you'll need stronger medicine.

### Privacy Badger Is Not An Ad Blocker

Sometimes, Privacy Badger is discussed alongside ad blockers like Adblock Plus. However, be sure to highlight that Privacy Badger is *not* an ad blocker. Instead, it's a *tracker blocker*. Privacy Badger blocks third parties that appear to be tracking you across the web, whether they're serving ads or not. Similarly, Privacy Badger will only block ads if they appear to be tracking you nonconsensually (see EFF's Do Not Track policy for more info.) In this way, one of Privacy Badger's goals is to encourage more responsible, transparent advertising that respects users' privacy.

### HTTPS Everywhere Doesn't Encrypt Everything

With HTTPS Everywhere, it's tempting for people new to the tool to think that it creates HTTPS where there is none.  You can clear this up by explaining that it's up to a website's administrators to decide whether or not their site offers HTTPS (and, luckily, more and more are offering it every day!). HTTPS helps after website administrators  turn on HTTPS. Some websites, even after turning HTTPS on, don't have HTTPS as the default, only encrypt some content, or still link to unencrypted pages. HTTPS Everywhere helps with these more complicated instances and makes sure that users get any HTTPS that would otherwise fall through the cracks. Users that want *all* their browsing to be encrypted can check the option "Block all unencrypted requests." It's important to know that this will make sites that offer *only* insecure HTTP connections unavailable, though.

### Internet Connectivity, and Other Installing Problems

Installing browser extensions is one of the simpler ways to install additional software, but it's still not foolproof. You may want to check connectivity with the venue beforehand, and stagger when and how people are downloading. If you're doing a survey or pre-event instructions, ask people what browser they use. You might even encourage advanced users to install the software beforehand.

## Anticipated Questions and Answers

To brush up on answers to frequently asked questions for HTTPS Everywhere, check https://www.eff.org/https-everywhere/faq.

Refresh your memory by reading Privacy Badger's Frequently Asked Questions as well: https://www.eff.org/privacybadger#faq.

### Learning Objectives

Learners will:

- Be able to explain how **HTTPS** is different from HTTP.
- Be able to explain the "third-party" in "third-party cookie."
- Install HTTPS Everywhere.
- Understand that HTTPS Everywhere does not create HTTPS connections when the website does not offer HTTPS.
- Install Privacy Badger.
- Understand that while Privacy Badger does block tracking, it should not be considered an "ad blocker."
- Optional: Gain exposure to browser fingerprinting and third-party tracking by using Panopticlick.

### Prerequisites

- Learners have their computers with them.
- Learners have a **web browser** (Firefox, Firefox for Android, Opera or Google Chrome) installed.
- Learners understand what a web browser is (and do not confuse it with a search engine or the Internet itself).

### Ratio

Instructor: Learners
One instructor to ten learners or more

### Suggested Materials

The instructor may want a computer and a projector to demonstrate the tools, and to show features of the browser extensions.

### Relevant Articles

This session is mostly a knowledge-share. You can have a one-to-many model for most of the session.

The installation process is only a few clicks, but some people may need to troubleshoot. During the installation portion, you can ask learners who were able to quickly install HTTPS Everywhere and Privacy Badger on their computers to help others who are having more trouble.

## Lesson Content

## Warm-Up Question

Have you ever seen those creepy ads on one site that seem to know what you have been browsing or purchasing on another site? Any stories of when an ad seemed to know something about you?

Do you ever notice the green lock symbol in your navigation bar? Any ideas as to what this green lock indicates?

## Knowledge Share

Before leading installation of Privacy Badger and HTTPS Everywhere, it might be helpful to go over:

### What is a browser, and why should I download these browser extensions?

Some examples of browsers are Firefox, Google Chrome, Safari, and Internet Explorer. Often, your computer comes with a browser already on it. The browser is how to connect to the Internet: you use it when you want to go to websites and browse the web. A lot of browsers have built-in security and privacy features. When you install these extensions, you are adding to those protections.

### Who is EFF and why should I download their stuff?

The standard answer is along the lines of: The Electronic Frontier Foundation is a San

Francisco-based nonprofit organization defending civil liberties in the digital world, including privacy, security, free speech, and innovation. Depending on your audience, you can tailor this to how it is relevant to them. You might explain your own experience with the organization, or issues EFF works on that are particularly relevant to you or your audience. (In the context of installing new software, emphasizing the non-profit, consumer-rights side of EFF's work often helps.) You also may want to emphasize that the extensions are **open-source**, so users can inspect the code that is running to ensure it isn't doing anything unexpected, or suspect, on their computers.

Downloading these two extensions is among the easiest digital security moves one can make. Once you install them, the extensions do most (if not all!) of the work for you to make sure that you are not tracked across the web and that you use a secure connection whenever possible.

## What does Privacy Badger do?

**Third-party tracking**—that is, when advertisers and websites track your browsing activity across the web without your knowledge, control, or consent—is an alarmingly widespread practice in online advertising. Privacy Badger puts you back in control by spotting and then blocking third-party domains that seem to be tracking your browsing habits.

Unlike other tracker blockers, which maintain a big list of trackers, Privacy Badger determines what sites to block by observing behaviors that are unique to trackers. Although Privacy Badger blocks many ads in practice, it is more a privacy tool than a strict ad blocker. Privacy Badger encourages advertisers to treat users respectfully and anonymously rather than the industry status quo of online tracking. It does this by unblocking content from domains which respect EFF's Do Not Track policy, which states that the participating site will not retain any information about users who have expressed that they do not want to be tracked. You can always click on the extension to see which sites are being detected and blocked, and change what is being blocked if you want to.

## What does HTTPS Everywhere do?

A collaboration between EFF and the Tor Project, HTTPS Everywhere is an extension for Firefox (both desktop and Android), Chrome, and Opera that makes your browser use HTTPS to encrypt its communication with websites wherever possible. Some websites offer inconsistent support for HTTPS, use unencrypted HTTP as a default, or link from secure HTTPS pages to unencrypted HTTP pages. Additionally, when a user types "example.com" into their browser, the browser will (for most sites) try connecting to the insecure HTTP version of the site, and only upgrade the connection if the site redirects it to HTTPS. This makes browsers vulnerable to attacks that take advantage of this redirect (e.g. SSLstrip). HTTPS Everywhere fixes these problems by rewriting requests to these sites to HTTPS, automatically activating encryption and HTTPS protection that might otherwise slip through the cracks.

To do this, HTTPS Everywhere maintains the largest list available of sites that support HTTPS, and is used by other software such as the Brave browser and Automatic HTTPS Rewrites. It is also included in the Tor Browser, to ensure that your anonymous browsing is as secure as possible.

## What is HTTPS, anyway?

There are two ways for a website to get to your browser: HTTP and HTTPS. The difference is that "S," which stands for "secure." Web pages that come to you over HTTP are vulnerable to eavesdropping, content injection, cookie and credentials stealing, targeted censorship, and other problems. HTTPS pages, however, come secure by default.

When you see “https” and a little green lock next to the web page address in the top of your browser, that means you are using a secure connection. You have probably seen this when shopping online or entering credit card information.

If someone is spying on the network and trying to see what websites users are visiting, an HTTP connection offers no protection. An HTTPS connection, on the other hand, hides which specific page on a website you navigate to--that is, everything “after the slash.” For example, if you are using HTTPS to connect to www.eff.org/ssd, an eavesdropper can only see “www.eff.org”. With HTTPS, an eavesdropper cannot see what part of a website you’re visiting.

### Activity: Installation!

Have your participants navigate to https://www.eff.org/privacybadger and https://www.eff.org/https-everywhere, and direct them to click on the button that corresponds to the browser(s) they use. At this point, some might need help identifying their browser. You can help with this and, as some people complete their own installation, you can ask them to circulate and help others, too.

### Activity: Visit Panopticlick

Learners who wish to check how well their browser add-ons are protecting them can visit https://panopticlick.eff.org/. If a learner has installed Privacy Badger during the session, they will see that their protection against trackers has been upgraded. You can also encourage the learners to run the test on the browsers of friends and family to see how well those browsers are protected. If their friends or family are insufficiently protected, the learner can then install Privacy Badger on that browser.

## For those in the audience who want to learn more...

About non-consensual third-party tracking:

New Cookie Technologies: Harder to See and Remove, Widely Used to Track You

How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them)

Browser Versions Carry 10.5 Bits of Identifying Information on Average

About Do Not Track, a complement to Privacy Badger in encouraging responsible, non-creepy advertising:

Understanding EFF's Do Not Track Policy: A Universal Opt-Out From Tracking

New Twitter Policy Abandons a Longstanding Privacy Pledge

Twitter (and Others) Double Down on Advertising and Tracking

Privacy Badger Makes Twitter a Little Less Creepy

About EFF’s initiative to Encrypt the Web:

Encrypting the Web

"Encrypt the Web" video