What are Tracking Pixels and How Do They Work?

Archived: 2026-04-06 00:16:08 UTC

A tracking pixel is an HTML code snippet which is loaded when a user visits a website or opens an email. It is useful for tracking user behavior and conversions. With a tracking pixel, advertisers can acquire data for online marketing, web analysis or email marketing. With log file analysis, long data evaluation or using appropriate analytical tools, this data can be used for different purposes, for example retargeting.

What is a tracking pixel?

A tracking pixel (also called 1x1 pixel or pixel tag) is a graphic with dimensions of 1x1 pixels that is loaded when a user visits a webpage or opens an email. Because it is so small, it can hardly be seen by visitors of a website or email recipients. These tracking pixels are partly or fully designed to be transparent, or camouflaged in the background color of the website so that they don't stand out to users. Users are usually not supposed to see the tracking pixel. The focus is mainly on the processes that are initiated by downloading the tracking pixel.

Tracking pixels within the source code might look like this:

```
<img style=""position: absolute;" src=""Tracking">
```

```
<img style=""display: none";" src=""Tracking">
```

```
<img src=""Tracking" width=""0"" height=""0"">
```

The tracking pixel URL is the memory location on the server. When the user visits a website, the image with the tag is loaded from this server. Optical properties such as visibility, or a very small size are defined using the style attribute.

How does a tracking pixel work

The website operator or sender of an email adds the tracking pixel using a code in the website's HTML code or email. This code contains an external link to the pixel server. If a user visits the destination website, the HTML code is processed by the client – usually the user's browser. The browser follows the link and opens the (invisible) graphic. This is registered and noted in the server's log files.

In addition, various information about the user is also transmitted using this method. To some extent, combination with JavaScript is necessary in order to collect information about the operating system or browser type.

The following data can be acquired and analyzed with a tracking pixel.

- Operating system used (gives information on the use of mobile devices)
- Type of website or email used, for example on mobile or desktop
- Type of client used, for example a browser or mail program.
- Client's screen resolution
- Time the email was read or website was visited
- Activities on the website during a session (when using multiple tracking pixels)
- IP address (gives information on the Internet Service Provider and location)

Inserting a tracking pixel

Depending on the system, the installation of a tracking pixel differs. Sometimes this can be done via the content management system used, sometimes the pixel must be implemented directly in the source code of the e-mail or website.

Usually, the web analysis tools that require the implementation of the pixel, such as Facebook or Google Analytics, offer extensive implementation instructions.

Criticism of tracking pixels

Tracking pixels are often criticized by data protection advocates because they collect comprehensive data about the user, mostly without knowledge of the user. As the tracking pixel cannot be seen with the naked eye, and the common user does not recognize the meaning of the small graphic even when it is visible, the tracking pixel involves a transfer of information without consent. Based on this, critics argue that with tracking pixels, user

privacy is violated through the recording of a motion profile. The transmission of the IP address also makes it possible to match information to other information on the Internet, e.g., to a profile in a social network or forum.

Tracking pixels also simplify the work of spammers. Spammers can integrate tracking pixels in their spam mails in order to find out if an email address is valid. If the recipient opens the email and thereby loads the automated tracking pixel, the spammer receives a confirmation of the authenticity of the email address. As a result, the sending of spam messages increases.

Data protection and tracking pixels

According to GDPR, users must be informed that a website collects data. Users also have to be able to object to the tracking.

Advantages of tracking pixels

The use of tracking pixels is beneficial for website operators, SEOs and email senders. This is because they can use the information generated to improve their online offers, make them more user-friendly, and adapt the offers to the most commonly used browser types and versions.

Even more advantageous is the fact that tracking pixels are more effective than cache in browsers: The access to a page is still counted. If JavaScript is used, more information can be collected. This includes the screen resolution, plugins used, support of certain technologies by the browser, etc. It therefore becomes possible to differentiate between users and bots, as well as create user profiles. The IP address, visits by a certain user, and the properties of this user can be used to create navigation paths. For web analysis, however, the tracking pixel generally just forms the basis. Advanced technologies are required which are only realizable by specialized service providers.

Tracking pixels can also be beneficial in the analysis of sent email newsletters, because they show the opening rates of certain emails or newsletters through the user statistics data. Together with A/B tests, successful campaigns can thus be determined. From the recipient’s point of view, this has the advantage that newsletters in the future can be designed to be more relevant and interesting.

Countermeasures for users

There are a number of ways in which users can prevent their data being collected by tracking pixels:

- Set browser and email settings to be as restrictive as possible such that external graphics are only supported after permission, and HTML emails are not supported. Appropriate firewall settings can also be used to do this.
- Some browser extensions can be used to make tracking pixels visible.
- Anonymous surfing with the Tor Browser or use of proxy servers to prevent the download of tracking pixels.
- In order to prevent the collection of additional user data such as browser type or operating system, the support of scripts in the browser can be deactivated. However, this can restrict other functions on the internet under certain circumstances.

Importance for web analytics, advertising and SEO

Tracking pixels generally have similar functionalities as cookies. The tracks of the user are recorded by a file that is saved in the user's hard drive. However, more and more users are nowadays taking up measures to block cookies using the browser functions. Cookies therefore often provide incomplete data, and their use is at times blocked completely.

The tracking pixel is can be used as an alternative to the cookie as its use cannot be blocked by a normal browser. Even so, several browser extensions, plugins, and programs that enable blocking of tracking pixels and hence prevent a log file analysis exist. Tracking methods such as Canvas Fingerprinting, Event Tracking, or different hybrid methods are also being used increasingly and as with all tracking models, comprehensive changes to the websites are necessary – e.g., in data protection. In addition, user consent to allow the tracking with pixels must be obtained.

Web Links

- Definition Tracking Pixel
