Web beacon

From Wikipedia, the free encyclopedia

  (Redirected from [Web beacons](https://en.wikipedia.org/w/index.php?title=Web_beacons&redirect=no))

[Jump to navigation](https://en.wikipedia.org/wiki/Web_beacon#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Web_beacon#searchInput)

*This article is about the web tracking technique. For bugs in web software, see*[*software bug*](https://en.wikipedia.org/wiki/Software_bug)*.*

A **web beacon** (also called **web bug**, **tracking bug**, **tag**, **web tag**, **page tag**, **tracking pixel**, **pixel tag**, **1×1**[**GIF**](https://en.wikipedia.org/wiki/GIF), or **clear GIF**) is a technique used on [web pages](https://en.wikipedia.org/wiki/Web_page) and [email](https://en.wikipedia.org/wiki/Email) to unobtrusively (usually invisibly) allow checking that a user has accessed some content.[[1]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-1) Web beacons are typically used by [third parties](https://en.wikipedia.org/wiki/Third-party_developer) to monitor the activity of users at a website for the purpose of [web analytics](https://en.wikipedia.org/wiki/Web_analytics) or [page tagging](https://en.wikipedia.org/wiki/Web_analytics#Page_tagging).[[2]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-2) They can also be used for [email tracking](https://en.wikipedia.org/wiki/Email_tracking).[[3]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-3) When implemented using [JavaScript](https://en.wikipedia.org/wiki/JavaScript), they may be called **JavaScript tags**.[[4]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-4)

Using such beacons, companies and organizations can track the online behavior of web users. At first, the companies doing such tracking were mainly advertisers or [web analytics](https://en.wikipedia.org/wiki/Web_analytics) companies; later social media sites also started to use such tracking techniques, for instance through the use of [buttons](https://en.wikipedia.org/wiki/Button_(computing)) which act as tracking beacons.

There is work in progress to standardize an interface that [web developers](https://en.wikipedia.org/wiki/Web_developers) can use to create web beacons.[[5]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-W3C-5)



**Contents**

* [1Overview](https://en.wikipedia.org/wiki/Web_beacon#Overview)
  + [1.1Framing](https://en.wikipedia.org/wiki/Web_beacon#Framing)
  + [1.2Use by companies](https://en.wikipedia.org/wiki/Web_beacon#Use_by_companies)
* [2Email-tracking](https://en.wikipedia.org/wiki/Web_beacon#Email-tracking)
* [3The Beacon API](https://en.wikipedia.org/wiki/Web_beacon#The_Beacon_API)
* [4See also](https://en.wikipedia.org/wiki/Web_beacon#See_also)
* [5References](https://en.wikipedia.org/wiki/Web_beacon#References)
* [6External links](https://en.wikipedia.org/wiki/Web_beacon#External_links)

Overview[[edit](https://en.wikipedia.org/w/index.php?title=Web_beacon&action=edit&section=1)]

A web beacon is any of a number of techniques used to [track who is visiting a web page](https://en.wikipedia.org/wiki/Website_visitor_tracking). They can also be used to see if an email was read or forwarded or if a web page was copied to another website.

The first web beacons were small digital image files that were embedded in a web page or email. The image could be as small as a single pixel, and could be of the same color as the background, or completely [transparent](https://en.wikipedia.org/wiki/Transparent_pixels) (thus the name “tracking pixel”). When a user opens the page or email where such an image was embedded, they might not see the image, but their [web browser](https://en.wikipedia.org/wiki/Web_browser) or [email reader](https://en.wikipedia.org/wiki/Email_client) would automatically download the image, requiring the user's computer to send a request to the host company's [server](https://en.wikipedia.org/wiki/Server_(computing)), where the source image was stored. This request would provide identifying information about the computer, allowing the host to keep track of the user.

This basic technique has been developed further so that all sorts of elements can be used as beacons. Currently these can include visible elements such as graphics, banners or [buttons](https://en.wikipedia.org/wiki/Button_(computing)), but also non-pictorial [HTML elements](https://en.wikipedia.org/wiki/HTML_element) such as the [frame](https://en.wikipedia.org/wiki/Framing_(World_Wide_Web)), style, script, input link, embed, object, etc., of an email or web page.

The identifying information provided by the user's computer typically includes its [IP address](https://en.wikipedia.org/wiki/IP_address), the time the request was made, the type of web browser or email reader that made the request, and the existence of [cookies](https://en.wikipedia.org/wiki/HTTP_cookie) previously sent by the host server. The host server can store all of this information, and associate it with a [session identifier](https://en.wikipedia.org/wiki/Session_ID) or tracking token that uniquely marks the interaction.

**Framing**[[edit](https://en.wikipedia.org/w/index.php?title=Web_beacon&action=edit&section=2)]

The use of [framing](https://en.wikipedia.org/wiki/Framing_(World_Wide_Web)) added a new level of versatility to web beacons. Framing allows web pages to *refer* to content such as images or buttons or HTML elements that are located on *other* servers, rather than hosting this content directly on their own server. When a user sees the email or the web page, the user's email reader or web browser prepares the referred content for display. To do so it has to send a request to the third-party server to ask it to send the referred content. As part of that request, the user's computer then has to supply identifying information to the third-party server.

This protocol allows companies to embed beacons in content that they do not directly own or operate, and then use such beacons for tracking purposes. The beacons are embedded in an email or web page as images or buttons or other HTML elements, but they are hosted on a different server than the website where they are embedded, and it is to this third-party server that requests and identifying information is sent.

For instance, in the case of an advertisement that is displayed as an image on a web page, the image file would not reside on the page's host server, but on a server belonging to the advertising company. When a user opens the page, the user's computer will request to download the advertisement from the page's server, but will then be referred to the advertiser's server, and will request to download the image from the advertiser's server. This request will require the user's computer to supply identifying information about itself to the advertiser.

This means that a third-party site such as an advertiser can gather information about visitors to the main sites, such as a news site or a social media site, even if users are not clicking on the advertisement. Moreover, given that beacons are not just embedded in visible advertisements but can be embedded in completely invisible elements, a third party can gather such information even if the user is completely unaware of the third party's existence.

**Use by companies**[[edit](https://en.wikipedia.org/w/index.php?title=Web_beacon&action=edit&section=3)]

Once a company can identify a particular user, the company can then track that user's behavior across multiple interactions with different websites or web servers. As an example, consider a company that owns a network of websites. This company could store all of its *images* on one particular server, but store *the other contents* of its web pages on a variety of other servers. For instance, each server could be specific to a given website, and could even be located in a different city. But the company could use web beacons to count and recognize individual users who visit different websites. Rather than gathering statistics and managing cookies for each server independently, the company can analyze all this data together, and track the behavior of individual users across all the different websites, assembling a profile of each user as they navigate through these different environments.

Email-tracking[[edit](https://en.wikipedia.org/w/index.php?title=Web_beacon&action=edit&section=4)]

Web beacons embedded in emails have greater privacy implications than beacons embedded in web pages. Through the use of an embedded beacon, the sender of an email - or even a third party - can record the same sort of information as an advertiser on a website, namely the time that the email was read, the [IP address](https://en.wikipedia.org/wiki/IP_address) of the computer that was used to read the email (or the IP address of the [proxy server](https://en.wikipedia.org/wiki/Proxy_server) that the reader went through), the type of software used to read the email, and the existence of any cookies previously sent. In this way, the sender - or a third party - can gather detailed information about when and where each particular recipient reads their email. Every subsequent time the email message is displayed, the same information can also be sent again to the sender or third party.

["Return-Receipt-To" (RRT)](https://en.wikipedia.org/wiki/Message_Disposition_Notification) email headers can also trigger sending of information and these may be seen as another form of web beacon.[[6]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-6)

Web beacons are used by email marketers, [spammers](https://en.wikipedia.org/wiki/Spam_(electronic)) and [phishers](https://en.wikipedia.org/wiki/Phishing) to verify that an email is read. Using this system, they can send similar emails to a large number of addresses and then check which ones are valid. Valid in this case means that the address is actually in use, that the email has made it past spam filters, and that the content of the email is actually viewed.

To some extent, this kind of email tracking can be prevented by configuring the [email reader software](https://en.wikipedia.org/wiki/Email_client) to avoid accessing remote images. Examples of email software able to do this include the [Gmail](https://en.wikipedia.org/wiki/Gmail), [Yahoo!](https://en.wikipedia.org/wiki/Yahoo!), [Hushmail](https://en.wikipedia.org/wiki/Hushmail) and [SpamCop](https://en.wikipedia.org/wiki/SpamCop)/[Horde](https://en.wikipedia.org/wiki/Horde_(software)) [webmail](https://en.wikipedia.org/wiki/Webmail) clients; [Mozilla Thunderbird](https://en.wikipedia.org/wiki/Mozilla_Thunderbird), [Opera](https://en.wikipedia.org/wiki/Opera_(web_browser)), [Pegasus Mail](https://en.wikipedia.org/wiki/Pegasus_Mail), [IncrediMail](https://en.wikipedia.org/wiki/IncrediMail), [Apple Mail](https://en.wikipedia.org/wiki/Apple_Mail), later versions of [Microsoft Outlook](https://en.wikipedia.org/wiki/Microsoft_Outlook), and [KMail](https://en.wikipedia.org/wiki/KMail) mail readers.

However, since beacons can be embedded in email as non-pictorial elements, the email need not contain an image or advertisement or anything else related to the identity of the monitoring party. This makes detection of such emails difficult.[[7]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-7)

One way to neutralize such email tracking is to disconnect from the Internet after downloading email but before reading the downloaded messages. (Note that this assumes one is using an email reader that resides on one's own computer and downloads the emails from the email server to one's own computer.) In that case, messages containing beacons will not be able to trigger requests to the beacons' host servers, and the tracking will be prevented. But one would then have to delete any messages suspected of containing beacons, or risk having the beacons activate again once the computer is reconnected to the Internet.

The only way to completely avoid email tracking by beacons is to use a text-based email reader (such as [Pine](https://en.wikipedia.org/wiki/Pine_(email_client)) or [Mutt](https://en.wikipedia.org/wiki/Mutt_(email_client))), or a graphical email reader with purely text-based HTML capabilities (such as [Mulberry](https://en.wikipedia.org/wiki/Mulberry_(email_client))). These email readers do not interpret HTML or display images, so their users are not subject to tracking by email web beacons. [Plain-text](https://en.wikipedia.org/wiki/Plain-text) email messages cannot contain web beacons because their contents are interpreted as display characters instead of embedded HTML code, so opening such messages does not initiate any communication.

Some email readers offer the option to disable all HTML in every message (thus rendering all messages as plain text), and this too will prevent tracking beacons from working.

More recently, many email readers and web-based email services have moved towards not loading images when opening a hypertext email that comes from an unknown sender, or that is suspected to be spam email. The user must explicitly choose to load images. But of course beacons can be embedded in non-pictorial elements of a hypertext email.

Web beacons can also be filtered out at the server level so that they never reach the end user. [MailScanner](https://en.wikipedia.org/wiki/MailScanner) is an example of gateway software that can neutralize email tracking beacons for all users of a particular server.

The Beacon API[[edit](https://en.wikipedia.org/w/index.php?title=Web_beacon&action=edit&section=5)]

The Beacon API ([Application programming interface](https://en.wikipedia.org/wiki/Application_programming_interface)) is a candidate recommendation of the [World Wide Web Consortium](https://en.wikipedia.org/wiki/World_Wide_Web_Consortium), the standards organization for the web.[[8]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-8) It is a standardized set of protocols designed to allow web developers to track the activity of users without slowing down website response times. It does this by sending tracking information back to the beacon's host server after the user has navigated away from the webpage.[[9]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-9)

Use of the Beacon API allows tracking without interfering with or delaying navigation away from the site, and is invisible to the end-user.[[10]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-10) Support for the Beacon API was introduced into [Mozilla's Firefox](https://en.wikipedia.org/wiki/Firefox) browser in February 2014[[11]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-11) and in [Google's Chrome](https://en.wikipedia.org/wiki/Google_Chrome) browser in November 2014.[[12]](https://en.wikipedia.org/wiki/Web_beacon#cite_note-12)

See also[[edit](https://en.wikipedia.org/w/index.php?title=Web_beacon&action=edit&section=6)]

* [Do Not Track](https://en.wikipedia.org/wiki/Do_Not_Track)
* [Email fraud](https://en.wikipedia.org/wiki/Email_fraud)
* [Facebook Beacon](https://en.wikipedia.org/wiki/Facebook_Beacon)
* [Internet privacy](https://en.wikipedia.org/wiki/Internet_privacy)
* [Local shared object](https://en.wikipedia.org/wiki/Local_shared_object)
* [Quantcast](https://en.wikipedia.org/wiki/Quantcast)
* [Web analytics](https://en.wikipedia.org/wiki/Web_analytics)
* [Web storage](https://en.wikipedia.org/wiki/Web_storage)
* [Web visitor tracking](https://en.wikipedia.org/wiki/Web_visitor_tracking)

References[[edit](https://en.wikipedia.org/w/index.php?title=Web_beacon&action=edit&section=7)]

* 1. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-1) *Stefanie Olsen (January 2, 2002).*[*"Nearly undetectable tracking device raises concern"*](http://news.cnet.com/2100-1017-243077.html)*.*[*CNET News*](https://en.wikipedia.org/wiki/CNET_News)*. Retrieved May 23, 2019.*
  2. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-2) *Richard M. Smith (November 11, 1999).*[*"The Web Bug FAQ"*](https://w2.eff.org/Privacy/Marketing/web_bug.html)*.*[*EFF.org*](https://en.wikipedia.org/wiki/EFF.org)*Privacy Archive. Retrieved July 12, 2012.*
  3. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-3) *Richard Lowe Jr And Claudia Arevalo-Lowe.*[*"Email web bug invisible tracker collects info without permission"*](http://www.mailsbroadcast.com/email.bolts.nuts/about.web.bugs.htm)*. mailsbroadcast.com. Retrieved August 22, 2016.*
  4. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-4) Negrino, Tom; Smith, Dori. *JavaScript para World Wide Web*. Pearson Education, 2001. <https://napoleon.bc.edu/ojs/index.php/ital/article/viewFile/1771/1677> accessed 1 October 2015
  5. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-W3C_5-0) *Jatinder Mann; Alois Reitbauer (April 13, 2017).*[*"Beacon"*](http://www.w3.org/TR/beacon/)*. W3C Candidate Recommendation.*[*W3C*](https://en.wikipedia.org/wiki/W3C)*. Retrieved November 7, 2019.*
  6. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-6) See [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) memorandum [RFC 4021](https://tools.ietf.org/html/rfc4021).
  7. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-7) *David Berlind (September 26, 2006).*[*"Have you received any "traceable" PattyMail recently?"*](https://www.zdnet.com/blog/btl/have-you-received-any-traceable-pattymail-recently/3671)*. ZDNet. Retrieved July 12, 2012.*
  8. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-8) [Beacon W3C Candidate Recommendation 13 April 2017](https://www.w3.org/TR/beacon/)
  9. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-9) [Introduction to the Beacon API](https://www.sitepoint.com/introduction-beacon-api/)- Sitepoint.com, January 2015
  10. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-10) [Squeezing the Most Into the New W3C Beacon API](https://nikcodes.com/2014/12/16/squeezing-the-most-into-the-new-w3c-beacon-api/)- NikCodes, 16 December 2014
  11. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-11) [Navigator.sendBeacon](https://developer.mozilla.org/en-US/docs/Web/API/Navigator/sendBeacon) - Mozilla Developer Network
  12. [**^**](https://en.wikipedia.org/wiki/Web_beacon#cite_ref-12) [Send beacon data in Chrome 39](https://developers.google.com/web/updates/2014/10/Send-beacon-data-in-Chrome-39) - developers.google.com, September 2015

External links[[edit](https://en.wikipedia.org/w/index.php?title=Web_beacon&action=edit&section=8)]

* [The Web Bug FAQ](https://web.archive.org/web/20010729060646/www.eff.org/Privacy/Marketing/web_bug.html) from EFF
* [Why Digital Marketing](https://www.wizkey.co/why-digital-marketing) from Wizkey.co
* ["Did they read it?"](https://lwn.net/Articles/86893/) from the [Linux Weekly News](https://en.wikipedia.org/wiki/Linux_Weekly_News)
* [Trojan Marketing](http://bcn.boulder.co.us/~neal/privacy/trojanmarketing.html)
* [Slashdot on Web Bugs](http://yro.slashdot.org/yro/06/10/13/1623217.shtml)—[Slashdot.org](https://en.wikipedia.org/wiki/Slashdot.org) forum thread on blocking web bugs