# How to track pixel tracking your email and how to block them

The pixel tracking has been around for a long time, both in email and on web pages. They are condemned for stealthily collecting data and often do not inform users that they are sending any information back to the server.

Do you know that something about the message 'Do you want to send a read receipt?' Do you receive it occasionally when opening an email? It is reasonable to assume that if you do not notice the message, no information will be sent back to the sender. But that is not always true.

Thanks to the magic of what is called tracking pixel (tracking pixel - a small image embedded in HTML and / or JavaScript), just opening the email can tell the sender not only when you opened the email, but also both the IP address (synonymous with location), the email client and the operating system you use.

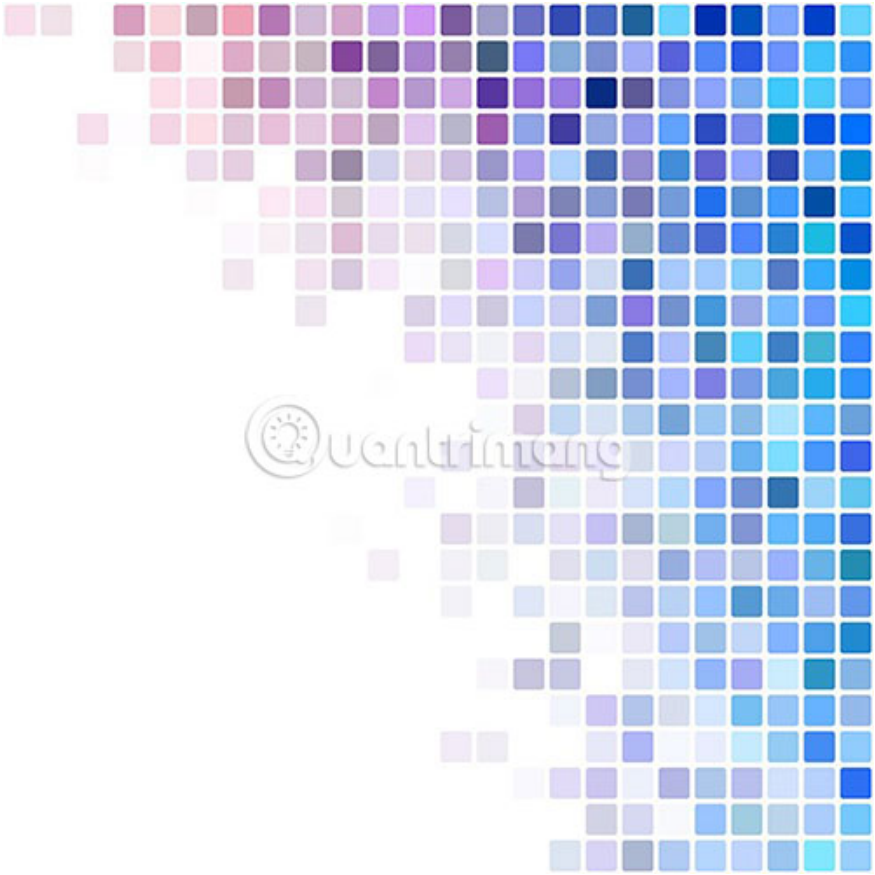

The pixel tracking has been around for a long time, both in email and on web pages. They are condemned for stealthily collecting data and often do not inform users that they are sending any information back to the server. Not just for companies, this technology is provided free of charge for individuals to use, allowing people to find other people's locations, by sending emails with the clickbait subject line (attractive, enticing). recipient clicks on) and a tracking pixel.

## Learn about tracking pixels

1. What is tracking pixel and how do they work?
2. Tracking pixel in email
3. Tracking pixel on the web
4. Can I block tracking pixels?

## What is tracking pixel and how do they work?

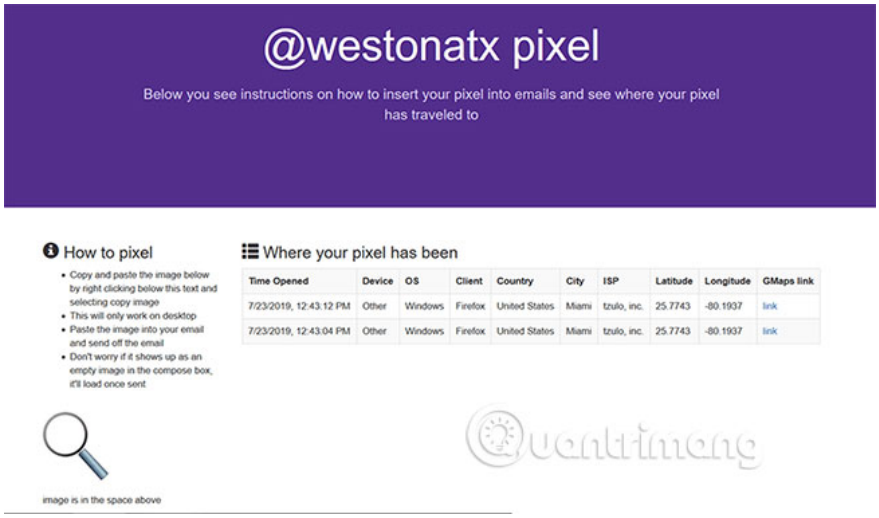
Tracking pixels are 1 × 1 image pixels (like GIF, JPEG, PNG, etc.), embedded in email or web pages like any other image, except that it is hidden. The pixel itself is already quite small, plus making the image transparent, blending it with the background or manipulating some code, you can make the tracking element essentially invisible. However, in essence, it is still an image, so when you open something with tracking pixel in it, your browser or email application will send a request to any server that tracking pixel is saved. stored on it.



When the server receives this request, it will record (at least) the time, date and IP address of the device that requested the pixel. If it is in an email, that log information can be used as a detailed message about reading emails. If the pixel is on a web page, it will return your IP address (and possibly other behavior information) back to any server it is hosted on, then be used to Traffic analysis and / or to help build more detailed profiles about you.

## Tracking pixel in email

Personal messaging tracking is probably the most controversial application for tracking pixel, as it makes people feel quite 'creepy'. A specific situation is as follows: Superhuman, an email client, has been condemned when building an automated tracking pixel system, letting users know when and where their mail is opened. This feature has not been removed, but is disabled by default and deletes location data.




Supertracker is a pixel tracking tool designed to show you how easy it is to keep track of people.

However, you don't need to be a Superhuman user to set the pixel tracking to your email. You can even try a demo created by a quick engineer, after the Superhuman scandal (reference link: http://supertracker.delian.io/).

Tracking personal messages in this way certainly makes many people feel that privacy is violated, but marketing emails are not used to track or evaluate how long we wait to respond, after open an email. They mainly try to optimize communication strategies only.

If you are trying to refine your email marketing (or find good spam targets), being able to get this type of data from tracking pixels is really too good and companies won't stop this. .

However, if you don't like to receive spam, be aware that loading images (or even other HTML elements) in spam emails may trigger tracking pixels, notify the spam server that you are human Use active email and clicked on spam. As a result, you will receive more spam! In addition, spammers know where you live.

# Tracking pixel on the web

Knowing that email is revealing a lot of information can be shocking, but the fact that websites are tracking users pretty much may be less surprising. Pixel tracking is just one of many tracking methods that websites use with cookies. You can see them used in many popular analytics and advertising targeting tools.

```
<!-- Facebook Pixel Code -->
<script>
  !function(f,b,e,v,n,t,s)
  {if(f.fbq)return;n=f.fbq=function(){n.callMethod?
  n.callMethod.apply(n,arguments):n.queue.push(arguments)};
  if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
  n.queue=[];t=b.createElement(e);t.async=!0;
  t.src=v;s=b.getElementsByTagName(e)[0];
  s.parentNode.insertBefore(t,s)}(window, document,'script',
  'https://connect.facebook.net/en_US/fbevents.js');
  fbq('init', 'your-pixel-id-goes-here');
  fbq('track', 'PageView');
</script>
<noscript>
  <img height="1" width="1" style="display:none"
       src="https://www.facebook.com/tr?id=your-pixel-id-goes-here&ev=PageView&noscript=1"/>
</noscript>
<!-- End Facebook Pixel Code -->
```

For example, Facebook pixels allow websites to connect to Facebook's advertising functionality, by embedding tracking pixels to enable visitor's IP address and browsing activity, then send it back to Facebook. Facebook can use that data to find your profile and offer ads. Most likely, Facebook is not the only company doing this. Pixel tracking is quite common in advertising analysis and targeting companies, specializing in collecting and brokerage of user data.

# Can I block tracking pixels?


Based on email tracking, the main remedy is to make sure your email application is set up to ask before loading external images. The catch is that you have to say no to all the images in the email (though, you might actually want to see some pictures in it). If you wish, you can disable HTML in your email. Some providers and clients allow you to do this.

Also, if you use Gmail (and only Gmail), you can consider Ugly Email or Pixelblock, which are Chrome extensions that help detect and disable tracking in email without blocking the Other images.

On the web, things are more complicated. Web beacons (one of many different techniques used on websites and emails, usually invisible, allow checking whether users have accessed certain content). designed to be very hard to find. Although extensions that protect privacy like Ghostery and Privacy Badger can catch some beacon webs, but not all.

GDPR may require websites to consult before monitoring you, but compliance with this is not consistent, depending on the user area. In any case, some monitors may pass any screen asking for permission from the user, so to keep the browsing really private, you will have to use at least VPN and Tor.

You finished reading the article "**How to track pixel tracking your email and how to block them**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.