Tracking pixels and how to block them

29 December 2025

In practice, individuals raise questions about how organizations determine that a person has read an e-mail sent to them or know the person's behavior while using an application. This information becomes accessible when tracking pixels are used. So, what exactly is a tracking pixel, and how can an individual block its use? **A tracking pixel**[1] is a reference to a resource, usually an image file, embedded into content such as a website, e-mail, or online advertisement. The purpose of this pixel is to collect information about users' behavior. The code portion of the tracking pixel contains an external reference address to the pixel's server. When a person visits a website or opens an e-mail containing a tracking pixel, the HTML code is processed, which, based on the reference, contacts the server and loads the pixel's graphic. Each time the server receives a request, it records this in log entries. In this manner, data about individuals' behavior is processed.

[1] European Data Protection Board Guidelines No. 2/2023 of 7 October 2024 on the technical scope of application of Article 5(3) of the ePrivacy Directive

When using a tracking pixel, the following data may be collected and analyzed:

- IP address
- Geographic location
- Type and version of the browser or e-mail application
- Type of device used (mobile or stationary)
- Screen resolution
- Operating system used and its version
- Time and frequency of visits
- Plugins used
- Behavior on the website, social network, or e-mail
- When the e-mail was read or the website was visited

Additionally, please note that tracking pixels in e-mails do not collect information about the recipient's e-mail address. However, in cases where an e-mail is not sent directly but is forwarded from a known sender, the original sender may obtain the new recipient's e-mail address. By using the tracking pixel and detecting a new active recipient, the original sender can see the new recipient's e-mail address from the e-mail's technical description.

How to block tracking pixels

Although tracking pixels may be invisible to individuals and in practice there are cases where users are unaware of their use because they were not properly informed about such data processing, there are several simple ways to block tracking pixels.
Tracking pixels received via e-mail can be blocked by disabling automatic image loading. This prevents images, including tracking pixels, from loading automatically.

How to block tracking pixels and automatic image loading in Outlook e-mail

1. Open Outlook (e-mail application)**.**

2. Go to Settings:

- Click **File** → **Options**.

3. Select Trust Center:

- On the left, select **Trust Center.**
- Click the **Trust Center Settings** button.

4. Open Automatic Download:

- Check the **Do not download pictures automatically in HTML e-mail messages or RSS items** option.
- Additionally, you may check **Warn me before downloading content when editing, forwarding, or replying to e-mail.**
- This will prevent images (including **tracking pixels**) from loading automatically.

5. Save the changes:

- Click **OK** → **OK** and close the settings window.

How to block tracking pixels and automatic image loading in Outlook Web App (using a browser)

1. Open Outlook (e-mail application) / log in to Outlook.com in the browser.

2. Go to Settings:

- Click **Settings** in the top right → click **View all Outlook** settings.

3. Select Mail → Compose and Reply:

- Scroll down to the **Message format** section.

4. Disable automatic image display:

- Mark **Don't automatically download pictures from the Internet**.

How to block tracking pixels and automatic image loading in your Gmail inbox

1. Open the Gmail inbox:

- Log in to your account at gmail.com.

2. Go to settings:

- Click **Settings** in the top right → click **See all settings**.

3. Find the Images section:

- In the **General** tab, scroll down to **Images**.
- Select **Ask before displaying external images**.

4. Save the settings:

- At the bottom, click **Save Changes**.

How to block tracking pixels and automatic image loading in browsers

1. **Using privacy protection extensions**, for example: *uBlock Origin*, *Privacy Badger*, *Ghostery*, *AdGuard*.
2. **Enabling the browser's built-in tracking protection:**

a. In the **Firefox** browser, the **Enhanced Tracking Protection** function is enabled by default. To check or change settings, open **Settings**, then select **Privacy & Security**, and then **Enhanced Tracking Protection**. Finally, select **Strict** mode.

b. The **Safari** browser has the built-in **Intelligent Tracking Prevention** function.

c. In the **Microsoft Edge** browser, the **Tracking Prevention** function can be used. To ensure maximum protection, select **Strict** mode.
