Stop Pixel Tracking

How to shut out tracking advertisers

They use email to hide tricky microscopic pixels

It's impossible not to be tracked online. Still, you can take steps that make a difference.

If you don't like the idea of advertisers knowing everything about you, shut them out.

When it comes to your email, you may not realize there's an easy way advertisers, marketers, companies, and even scammers track you – with just one tiny pixel.

What is pixel tracking?

You can't see them, but pixel trackers are hidden in many of the emails you receive. Technically, this microscopic pixel is computer code embedded within the body of an email, generally hidden within an image.

Typically, pixel-tracking allows marketers, advertisers, and companies to collect data about you, such as:

• The number of times you open an email
• The operating system you use
• The time you opened the email
• Your IP address can give an idea of your location
• What type of device you use to open the email Detailed data is sent back to the sender automatically, without you having to click on any links or even respond. That may feel like an invasion of privacy, but it is legal and different from when hackers and scammers employ this tactic.

In that case, it becomes all about monitoring your activity.

Speaking of monitoring, spyware is dangerous software that tracks everything from the sites you visit to the passwords you type in.

Pesky marketing emails are one thing, and we will get into how to stop that.

But first, let's review the red flags you should send an email straight to the trash:

• There's a request for personal information.
• The "From" address and the display name don't match.

Stop Pixel Tracking

• The “From” address is very similar to a known business or contact, with one or two characters changed.
• It requires immediate attention.
• It is full of poor spelling or grammar. (Often, this feels like something is “off.”)
• There’s a request to click on a link or download a document or file you did not request.

Most of these clues are easy to spot, but you won’t see a microscopic pixel hidden in an email.

Apple automatically stops senders from retrieving your IP address starting with iOS 15, macOS Monterey and iPadOS 15.

Additionally, email content is downloaded privately when you receive the email, not when you view it. That means only generic data is sent back to marketers, companies, and anyone else tracking you via email.

The Mail Privacy Protection features are not enabled by default. Here’s how to turn them on:

• On an iPhone or iPad: Go to Settings > Mail > Privacy Protection. Turn on Protect Mail Activity.
• On a Mac: In the Mail app, choose Mail > Preferences, then click Privacy. Select Protect Mail Activity.

The simplest way to prevent pixeltracking is to block images from displaying in your emails. If the pixel isn’t displayed, the code probably won’t work.

• In Gmail on a computer: Click on the gear icon and select See All Settings. Under General, scroll down and click on Ask before displaying external images under the Images option. Click Save Changes at the bottom of the page.
• In the Gmail app: Tap the three-line menu in the upper corner > Settings > Choose your account. Scroll down to Images under Data usage. Click it, then choose Ask before displaying external images.
• In Yahoo Mail: Click Settings > More Settings > Viewing Email. Scroll to the bottom. Under Show images in messages, choose Ask before showing external images. The page will refresh and automatically save.

Stop Pixel Tracking

• In Outlook, click on File > Options >
Trusted Center. Choose Trust Center Settings > Automatic Download from the left-hand pane. Select Don't download pictures automatically in HTML e-mail messages or RSS items. Click OK to save.
Want smart tech tips like this straight to your inbox? Try my free Tech Tips and How-tos newsletter. I'll help you get the most out of all your gadgets, save money and protect your privacy.
Learn about all the latest technology on the Kim Komando Show, the nation's largest weekend radio talk show. Kim takes calls and dispenses advice on today's digital lifestyle, from smartphones and tablets to online privacy and data hacks. For her daily tips, free newsletters and more, visit her website at Komando.com. The views and opinions expressed in this column are the author's and do not necessarily reflect those of USA TODAY.

Speaking of monitoring, spyware is dangerous software that tracks everything from the sites you visit to the passwords you type in.

You can't see them, but pixel trackers are hidden in many of the emails you receive. GETTY IMAGES

Tech Talk Kim Komando

Since tracking pixels work by loading remote images in an email when the receiver opens the message, you simply need to configure your email client to not load remote images by default. Doing so will ensure a tracking pixel can't send code back to the sender's server alerting them you've read their email.

Stop Pixel Tracking

Here's how to block tracking pixels in the most popular email services and email clients:

- macOS Mail app: go to Mail>Preferences>Viewing and uncheck "Load remote content in messages."
- iOS's Mail app: go to the Settings app, tap Mail, then toggle the "Load Remote Images" switch to OFF (white).
- Gmail on the web: Log into your Gmail account, then click the Settings (cog) icon. Now click Settings. On the Settings screen under the General tab, scroll down to the Images section and make sure "Ask before displaying external images" is selected.
- Android Gmail app: in the Gmail app, select your account, tap on Images, and then select "Ask before showing."
- Outlook email client: Microsoft has disabled loading remote images by default—a wise move. To make sure it's still disabled, open Outlook and choose Options > Trust Center. Under Microsoft Outlook Trust Center, click Trust Center Settings. Make sure the "Don't download pictures automatically in HTML email messages or RSS items" checkbox is checked.

There are also a number of Chrome and Firefox browser extensions that will alert you if a tracking pixel is detected in an email you have opened in a browser window, the most popular of which is Ugly Email.