www.fastcompany.com

How to stop email trackers from spying on you

Make no mistake about it: Companies want to know everything you do online, whether it's when you post to social media, or what subject you're reading about on Wikipedia. Shadowy data brokers, big tech giants, your ISP, even your local car dealer can tap extensive data on you based on your digital footprint.

As tracking techniques get more advanced each year, so do the methods to thwart such attempts. There are literally dozens of browser extensions built to help protect users from tracking–and entire browsers themselves. But while it's generally known by most people that our online activities–where and what we browse–are being tracked in some way, not many people realize that companies have been using a sneaky hidden trick for decades that allows them to snoop on your email activity.

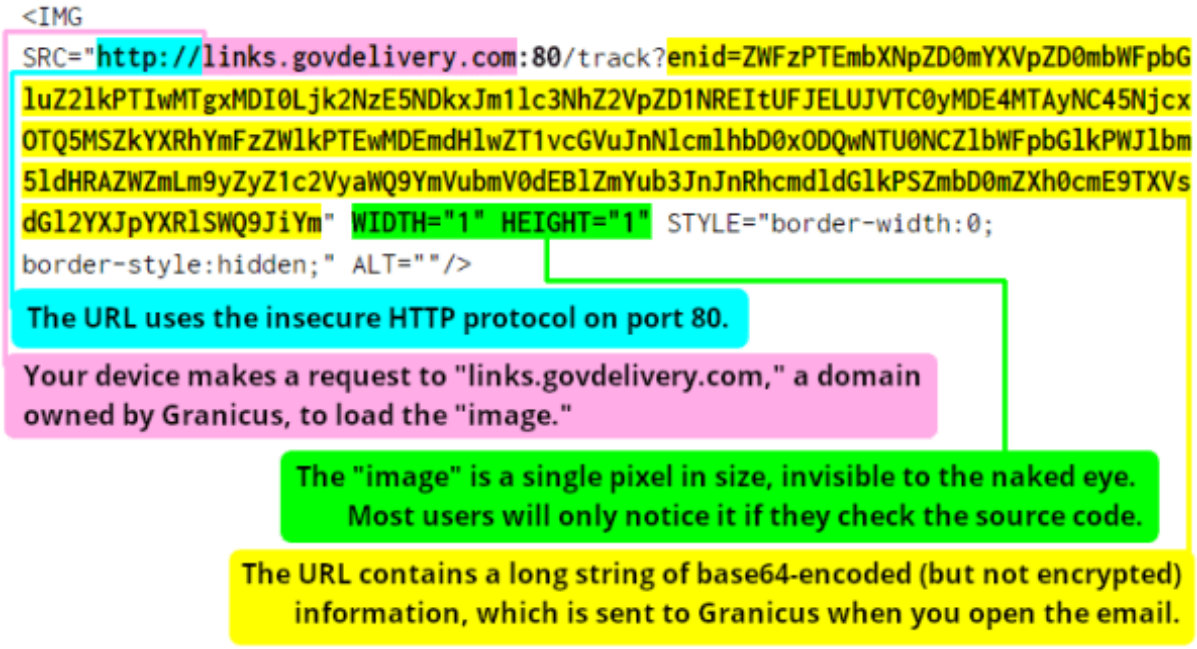
This email tracking allows a company–or virtually anyone–to see when and where you've opened an email they've sent you, how long it took for you to read it, and how often you've returned to read the email again. They do this through a snooping trick called a tracking pixel.

How tracking pixels work

Tracking pixels are usually an invisible image file that measures 1 pixel high by 1 pixel wide that is inserted without your knowledge into an email sent to you. The tracking pixel contains code that, when the email is opened, will send data back to the company's server that tells them exactly what time you read the email, how long you spent reading it, and, many times, even the location you were at when you read the email.

Tracking pixels work by leveraging basic HTML technology. While most emails we send to and receive from friends are usually sent in plain text, emails from marketers and other companies generally have HTML-based images in them, such as the company logo or a picture of the company's products.

The images aren't actually embedded in the email itself; instead, they are displayed in the email once the email is opened and the HTML code tells your computer to retrieve the images from the sender's servers. It's this retrieval of the image files from the sender's servers that allow the sender to see exactly what time you opened the email.



A tracking pixel in an email sent to subscribers of the Whitehouse.gov email list in October 2018 by Granicus, a government contractor that provides email services to 4,000 government agencies, identified by the Electronic Frontier Foundation. [Image: EFF]Needless to say, tracking pixels are a boon to marketers, because when they send you an email (spam or otherwise), tracking pixels allow the marketer to see how many people have opened the email (and thus, that your email address is valid), and how long people have spent reading their messages.

Why tracking pixels are creepy

But despite being a great tool for marketers in an age when our digital privacy matters more than ever, it's clear tracking pixels are creepy for multiple reasons.

The first is that no one is ever offered an opt-in or opt-out to tracking pixels. Companies use them without getting your permission first and without your knowledge that they are even being used at all. Given this, why should companies have that right to see when you've read an email in the first place? If someone from the marketing agency was camped out in a tree in front of your house and using binoculars to peer through your windows to see if you're reading their email, we'd call that creepy. So how is using an invisible trick to spy on us to achieve the same goal not creepy?

It's also not just marketers that can use tracking pixels. Anyone can insert one into any email they send. And again, this tracking pixel will just be an invisible 1-pixel-by-1-pixel image. You won't know it's there. But by inserting the tracking pixel into your email, the person will be able to spy on a portion of your private life without you ever knowing.

And don't think this can't be abused. By using tracking pixels, a stalker could see when an object of his or her obsession has read their latest email screed. Further, and as already mentioned, not only can a tracking pixel let the stalker know when their email has been read, but what time it

was read, on what device it was read, and even the location in which it was read. Remember, because tracking pixels are invisible to the naked eye, an email you receive could look like it only has plain text when in fact it has a tracking pixel in it.

By the way, it's not just stalkers and marketing companies that love using tracking pixels. PR people love embedding them into emails they send journalists so they can tell if the journalist is choosing to ignore them.

How to block tracking pixels

If you're sufficiently creeped out now about tracking pixels, the good news is they are relatively easy to block–though most people don't.

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. 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.

One final word: While blocking remote images from loading will protect you from tracking pixels, it also means remote images won't be loaded in your emails by default. This can make emails from, for example, banks, look a bit jumbled. However, all the email services and clients listed above offer a one-click button in the email message itself that allows you to load remote images in that email only. Given this, there is no reason not to disable loading remote images by default

in all your email clients to protect you from tracking pixels.