Tracking email and privacy infringement - old problems that are not old

If you think you can lie about reading an email, but in fact, that thought is naive!

Have you ever thought about the existence of an application called 'Superhuman', which can track anyone through their email box?

It is also a problem that has been discussed in thousands of different large and small technology forums around the world, in parallel with the birth and development of email services. It is not clear whether you know it or not, but perhaps many people have heard about the story of an email application that offers a monthly 'email tracking' service. With only a small monthly payment, the app will give you the feature to automatically track each time the recipient sees the email you send them, and even provides you with the specific location of Real-time email recipients.

1. Be wary of disguised Microsoft OneNote Audio phishing emails

Track email

As expert Mike Davidson, Twitter's former vice president of design, shared on his personal blog, the application could do that because it's integrated hidden pixel monitors (pixel trackers). .

But anyway, we, who have to work with computers every day, have time to interact with technology even more to meet relatives, almost impossible to 'live without' email. Therefore, finding out how such cases like Superhuman are really applications and how they work is an interesting and essential idea.

Basically Superhuman can be turned on by default, keeping track of any objects you email, whether you intend to follow them or not. We will learn more about this application as well as email tracking through the following questions.

What are tracking pixels (tracking pixels) and can I use them as "professional spies"?

Do you know that all images on the internet can be stored on servers and your computer will automatically download them when you browse? Years ago, some computer geniuses discovered that requests to browse images on your computer could allow that image host to track your activity on the web. Similarly when sending emails, email storage servers can provide the sender with certain information about the recipient when they open the email.

1. The winning scam from Google: 'The cat game' for the vigilant, 'tragic' for those who are light-hearted

Tracking pixel can record quite a bit of your information

About the operation mechanism, it is not too complicated: When you open the email, you will automatically download the content (may include images, attachments) in the email, and the request for display Displaying those content immediately will let the server know that you have actually opened the email.

In a study that analyzed 1000 different emails, it was found that up to 70% of those emails contain ad trackers - which can automatically download components like invisible images (tracking pixel). These components not only provide the sender with information about when and the number of times you open the email, but in many cases they also transmit personal data in the query string. In addition, tracking domain queries can also indicate your IP address, thereby helping email senders identify your current location with a high degree of accuracy.

So, if you think you can lie about having read the email they sent, but in fact, that thought is naive.

Have you read my email yet? Please open the email!

1. Microsoft admits hackers may have read Outlook email and warned users to change their passwords

Do tracking pixels have any other names? What do they look like? How do I recognize their presence?

Wikipedia experts say they also call tracking pixels web beacons, web bugs, tracking bugs, web tags, page tags, pixel tags, 1 x 1 GIFs, and clear GIFs. With email, sometimes, this overall concept is called open tracking. It's an idea related to the 'read receipt' feature that you often see on messaging apps like Messages or WhatsApp.

You may have never seen tracking pixels before, and certainly not with the naked eye, because they can be a 1 x 1 pixel image buried somewhere in an email or web page. In fact, tracking pixels can also be embedded in the sender's avatar - or even the preferred font they use. Indeed, anything that sends a request to a remote server can be used as a tracking tool.

To make it easier to visualize how well tracking pixels can be 'hidden', think of pointing out where the four ninja are hiding in the picture below:

Can you see 4 ninja hiding?

So here, we almost can't recognize the presence of tracking pixels with the naked eye.

1. 25% of "out-of-the-box" phishing emails are the default security of Office 365

Are there other types of tracking pixels that are monitoring you?

That's probably the Google Pixel you are using with dozens of built-in user data collection tools inside it.

Many people said that this tracking technology was old and appeared long ago, so why are they still upset about its presence until now?

Probably in part because so many people don't really realize the existence of tracking pixels, this is not uncommon.

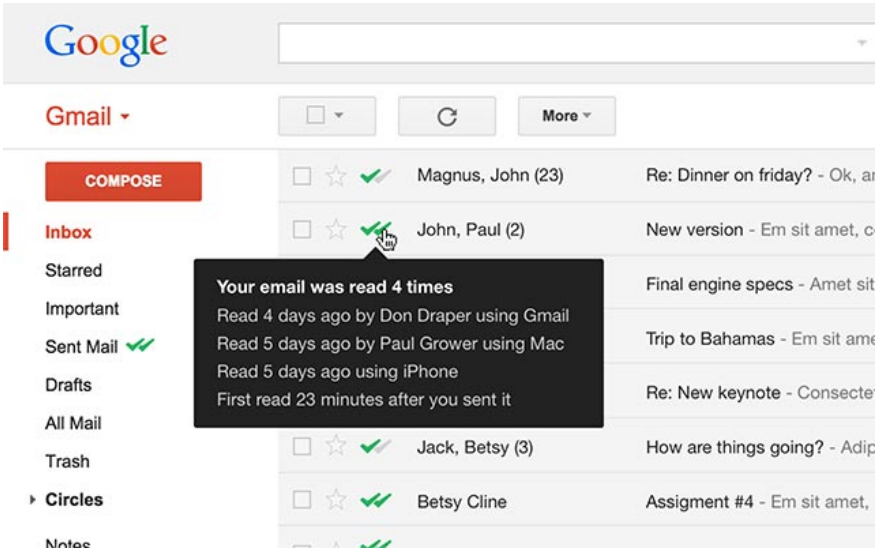
Perhaps in part because Twitter's former design director wrote a blog post on the issue and the post received a lot of buzz on Twitter.

Or maybe it's partly because Superhuman has allowed email senders to monitor information about recipients just by sending a brief message, and this 'feature' has been defaulted since the email was born.

Is it a good idea to know someone who has read the email you sent?

As stated above, read receipt in the message has many similarities with tracking pixel in the email in that it allows both senders and recipients to be able to see clearly whether their message has been read or ignored, From there may complain about the enemy deliberately ignoring the message or slow response. Socially speaking, this is relatively harmless.

1. 773 million emails, 21 million passwords were revealed on the Internet, this is the largest personal data leak in history



The sender can see how many times his email has been read and read

But Superhuman and the like are another story. Here we will have to say more about the situation where a stranger is able to track your location information just by sending anonymous emails. It is a violation of privacy, and it is harmful, in many situations.

How on earth did service companies know my location?

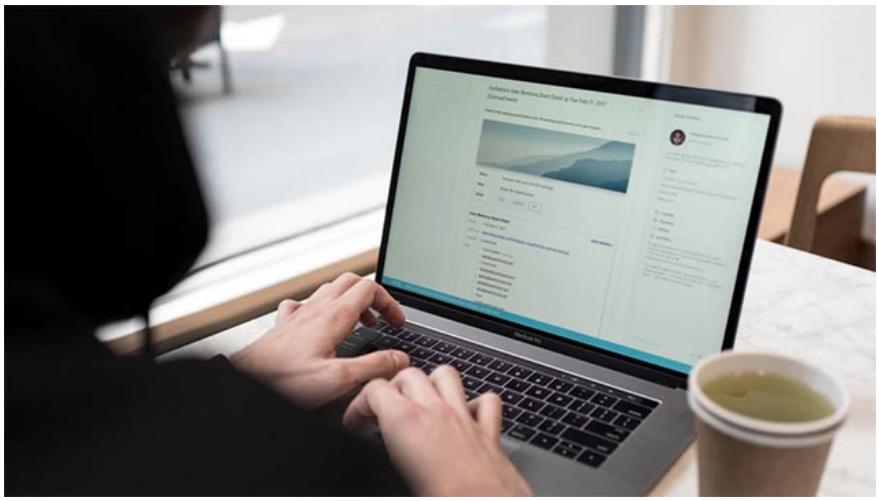
Based on the IP address, it is possible. When you download a tracking pixel from your service provider's server, it will record your IP address, which is how most Internet-based companies need to identify your computer. Where are they located, both geographically and digitally. It is possible to find out exactly the street address where you are accessing the network without having to use any other factors than the IP address, and here, at least we can talk about degrees. Exactly almost absolute at the provincial and city level.

How can this be abused?

A classic example: If the thief knows when you will have to go out and the time you go home, his job will become much easier. Similarly, spammers and phishers can use social engineering to know how the title lines can lure you to click on that spam email. As well as the countless people being tracked through email anonymously without knowing it.

1. Even if denied access, thousands of Android applications can still track you

Is Superhuman the only application doing this?



Tracking email is a common problem

Are you sure! Previously popular Wired technology magazine once published a great article on email tracking in 2017, in which the author specifically emphasized an application called Streak. This application has publicly provided email tracking for nearly 6 years. And just by searching for the keyword 'email tracking' on Google, you'll see the Streak or Superhuman is just the tip of the iceberg.

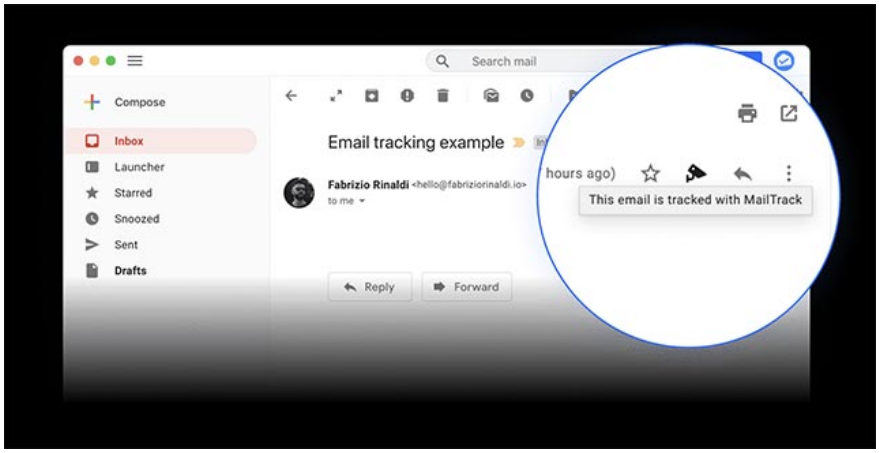
Is it legal to follow this email?

This is difficult to delineate clearly due to national regulations. However, Europe's current GDPR security regulation stipulates that before you want to collect personal data of an EU citizen, you must have their consent.

Can my email application block these pixel tracking?

There is good news for Gmail users: Google has rerouted all image requests through their own proxy servers. Tracking pixel will still provide information about when you read the email, but in general they can no longer be used to detect your location, or collect your advertising records as before, single Because they cannot see your IP or cookie (instead of Google IP).

1. [Infographic] Selecting a suitable messaging application for Enterprises



Email is being tracked

You can also turn off automatic image downloading in many email applications, then your email will not automatically download images, but this can be inconvenient in many situations. There are also browser extensions like Ugly Email and PixelBlock that provide the ability to detect pixel tracker before you open the email and delete them completely.

What about using ad blockers?

Sure, but you will need specific settings for each pixel tracker you want to block.

Why do big browser companies accept tracking pixels?

Perhaps because large web companies have used these trackers in their business and service systems for many years without leaving any problems too serious. Pixel Facebook, Google Tag Manager, and Pixel Amazon are the most obvious examples, but most of them are used on the web, not email. In terms of email, it is estimated that most newsletter services (such as MailChimp) own a basic tracking mechanism by default. Tracking pixels are often considered an indispensable part, just as tracking cookies often keeps a record of the websites you have visited.

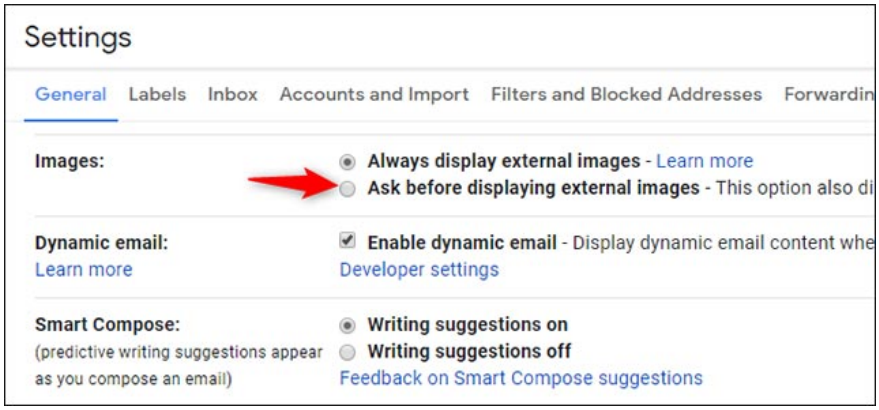
However, if we look on the positive side, in a post-Cambridge Analytica world, technology companies are increasingly making efforts to regain customer confidence, we have seen the emergence of browsers begin to be stern. More slots with cookies. The same case may also appear with tracking pixels.

1. Google Stadia - The name of the spy in the cover of the gaming service, maybe!

Can I use tracking pixel to deal with people trying to track me?

Sure. But do you want to participate in an exhausting 'arms race' without gaining any significant benefits like that?

How to prevent email tracking



Turn off auto-image loading to deal with tracking pixels

At the top, we talked about how to deal with tracking pixels, and now will be a way to prevent being monitored by email. Basically, there are 3 options that limit being tracked by email that you can apply, including:

1. Deactivate the feature to automatically load images in the email application, and set up to download only images from trusted senders.
2. Turning off the automatic loading of images will make the email look quite boring. If you do not want to do so, use a third-party monitoring tool, such as Private Browsing in Kaspersky Internet Security.
3. Use VPN, such as Kaspersky Secure Connection. VPN will help hide your real IP address, making it impossible for advertisers to collect IP addresses.

The above is just the most basic information about 'email tracking' - a problem that is not new but has never lost the topicality. Hopefully you are somewhat aware of the existence of this privacy threat and have the option of using email accordingly.

You finished reading the article "**Tracking email and privacy infringement - old problems that are not old**" 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.
