Why can GDPR warn of malicious websites?

GDPR stands for General Data Protection Regulation and aims to give people more control over their personal data.

You may not visit any website or online platform without receiving a pop-up asking you for permission to access personal information. New and upcoming privacy laws could help put an end to the amount of information websites can ask from you. They can also help you better detect fake and malicious websites.

So what is GDPR? And how can it keep you away from malicious websites?

What is GDPR?

GDPR is a privacy regulation from 2018 that applies to European and international companies operating in the region. GDPR stands for General Data Protection Regulation and aims to give people more control over their personal data.

GDPR-compliant companies and websites cannot collect any data without explicitly asking for permission. Although you can change your preferences later, if you accept the website's cookies, it will remember your preferences and not ask you when you visit the website again.

How can GDPR help you identify malicious websites?

Websites are GDPR compliant because they are required by law. But sites with shady origins and little or no legal documentation are rarely held to the same standards. For example, if a website you've never visited before doesn't ask you to provide a privacy preference, it could be a fake site.

Of course, not asking for permission can also mean that the site does not collect user data. However, in most cases, websites use cookies, so must comply with GDPR. One way to notice the difference is whether you interact with the site or change its settings - theme, font or by clicking a link - and whether the effects are still there when you visit again. or not.

The fact that you do not submit any credit card or password information does not mean that the website cannot collect valuable information about you. Cookies can store a variety of information you enter, such as your name, email address, and phone number. Persistent cookies (persistent cookies) can keep profiles of your login details, preferences, themes and bookmarks.

What should you do after visiting a fake website?

Start by clearing your browser's cookies and any traces the site might use to identify you the next time you visit that site, or one of its affiliated sites. If you have entered any sensitive information, especially if the site connection is not encrypted, change them as soon as possible.

Besides, get security software to scan for viruses or any malicious content.