**Know the Ways Your Data is Collected and How You Can Prevent This**

**Introduction**

While browsing the internet, you might have come across a popup on the website saying cookies notice. This is a tool that tracks your IP address and lets the website collect some information from you. Websites use various technologies to track your activities and to understand you. They collect data that can include the device you are using, your location, your contact details, advertisements you have watched, and more.



If the site is malicious and you are revealing your [IP address](https://www.expressvpn.com/what-is-my-ip), then the files stored in your system, your passwords and other personal information can be at risk. So, how can you hide your IP address? Well, for this, you don’t have to be tech-savvy as there are a few tools that can help you with this. All you need to do is use a VPN tool. Speaking about VPN, it functions by diverting your internet connection through your selected VPN server instead of your own internet service provider. When the data is transmitted, it will come directly from the VPN instead of your system. This way, the site won’t be able to track your IP address.

Should you let someone track your activity? Is your data safe with them? How can you prevent them from collecting data? Keep reading the article to know to get your answer. Let’s start by knowing why businesses or different parties collect your data?

**Why Do Different Businesses Collect Your Data?**

For all businesses, data has emerged as a crucial asset. They contextualize the data and get new valuable insight from it. Starting from consumer behaviour to predictive analytics, websites obtain, store, and process a considerable database every day. But why do they do that? It’s all about business growth. The [data they collect from you](https://www.globalsign.com/en/blog/what-data-is-collected-about-you-online), help them to refine their business. Here are some significant ways they use your data:

* **To enhance the customer experience**

Almost all the companies use customers' data to understand as well as fulfil the customer’s demand. They analyze the data to understand the customers' behaviour and nimbly modify the brand’s digital presence

* **Developing a marketing strategy**

Data contextualization helps businesses to know how people are responding to the marketing campaign and will develop the plan accordingly.

* **Converting the data into cash flow**

There are some companies, or you can say data brokers who buy and sell customers data and make a lot of money. They generally sell the data to advertisers or marketers.

**What types of data can a website collect?**

1. **IP address**

Your IP address lets the data collectors know about where you are browsing from as well as what ISP you are using right now. It can reveal your location to the tracker.

1. **Software as well as hardware details**

Your browser can send all types of information to the website you are visiting. This can include information about the computer system you are currently using. Besides, the site will read the operating system, GPU, and about the software you are using. This may seem normal, but it will reveal the ID of your machines.

1. **Cookies**

Speaking about cookies, it is one type of small file that a website installs on your system to track the things you are doing online. So, when you visit the site next time, it will know in advance what you are looking for. For the companies, this can be a good thing, but for you, it may not be a good thing.

1. **Invisible tackers**

Most of the new sites, as well as other popular sites often display advertisement content at the bottom of every page. Google also does this. This is the reason when you search for products on Google search engine, you will see ads related to that product on the site that has Google AdSense code.

1. **Autofill data**

Sometimes you might have noticed that when you are filling up shipping details on a new site, your browsers will automatically fill-up the form by inserting the details such as your shipping address, name, and more. It may sound very convenient but can also lead to a privacy nightmare.

Now let’s have a look at a certain situation where you reveal your data to websites.

**Case 1**

**Situation:** You all love posting photos or videos on the different social media platforms. But when you post the photos, it automatically generates data containing various personal information. For example, your current location, information about people tagged in the photos or videos, and more.

**Problem:** Now imagine a hacker who has hacked the posts and obtained all that invisible information about you. They can now keep an eye on you and can locate where you are right now. So, they can enter your house when you are not at your house.

**Solution:** Take extra care while posting on a social media platform and know what type of information you are revealing about. Always try to hide your IP address to hide your location.

**Case 2**

**Situation:** While buying goods online, you fill-up the payment details to carry out the payment. Some sites will prompt you to save the payment source details, like credit or debit card details, so that you can use them in the future.

**Problem:** Well, this is a good thing. What if the site is hacked and your card details are compromised? Hackers can use the card details to know your account number and can hack it without your notice.

**Solution:** The best thing that you can do to avoid such an incident is never storing your card or payment details on shopping sites. Besides, you need to make sure that the site has an SSL certificate.

**Case 3:**

**Situation:** You are using online photo editing tools to edit your photos. The site will generally ask you to upload your photos from Google Drive or the local system. When you upload the photos from these sources, the site will track it and store it on the site.

**Problem:** If the site is not highly protected, then hackers can get access to your Google Drive or Google Photos and can collect all the data.

**Solution**: While using such a platform, always use IP address blockers. Besides, prefer to use offline software as much as possible.

**Conclusion**

Online privacy has emerged as a major concern for all. You should be very careful about what type of information you are sharing knowingly or unknowingly. As discussed, your IP address, [domain name](https://www.website.com/beginnerguide/domainnames/8/1/What-is-a-domain-name?.ws), page visit information, the system as well as software details are saved on sites. Besides, companies can also use advanced technology to obtain more information like the browsing patterns, the site you are visiting, and more.

However, you need to be very careful while sharing your private information. Don’t reveal your debit or credit card information, address or password, unless you trust the site. Make sure that the site utilizes SSL for data encryption. Some sites may ask you to provide the social security number, for example, the websites related to financial services, think twice before that. You will not like it when someone breaks into your house when you are alone or not at your house.