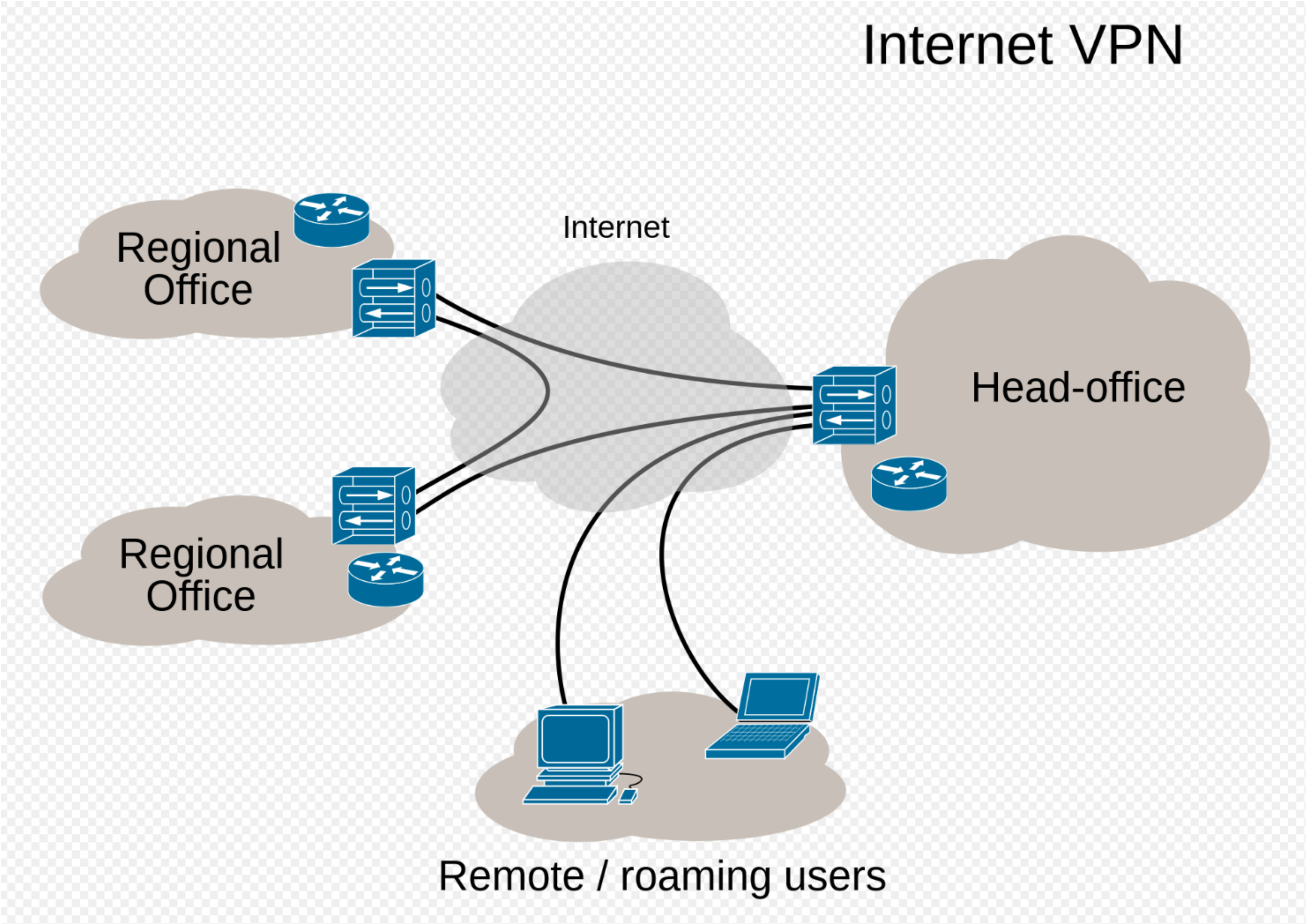
VPNs And Cookies In The UK

What are they and how do they work

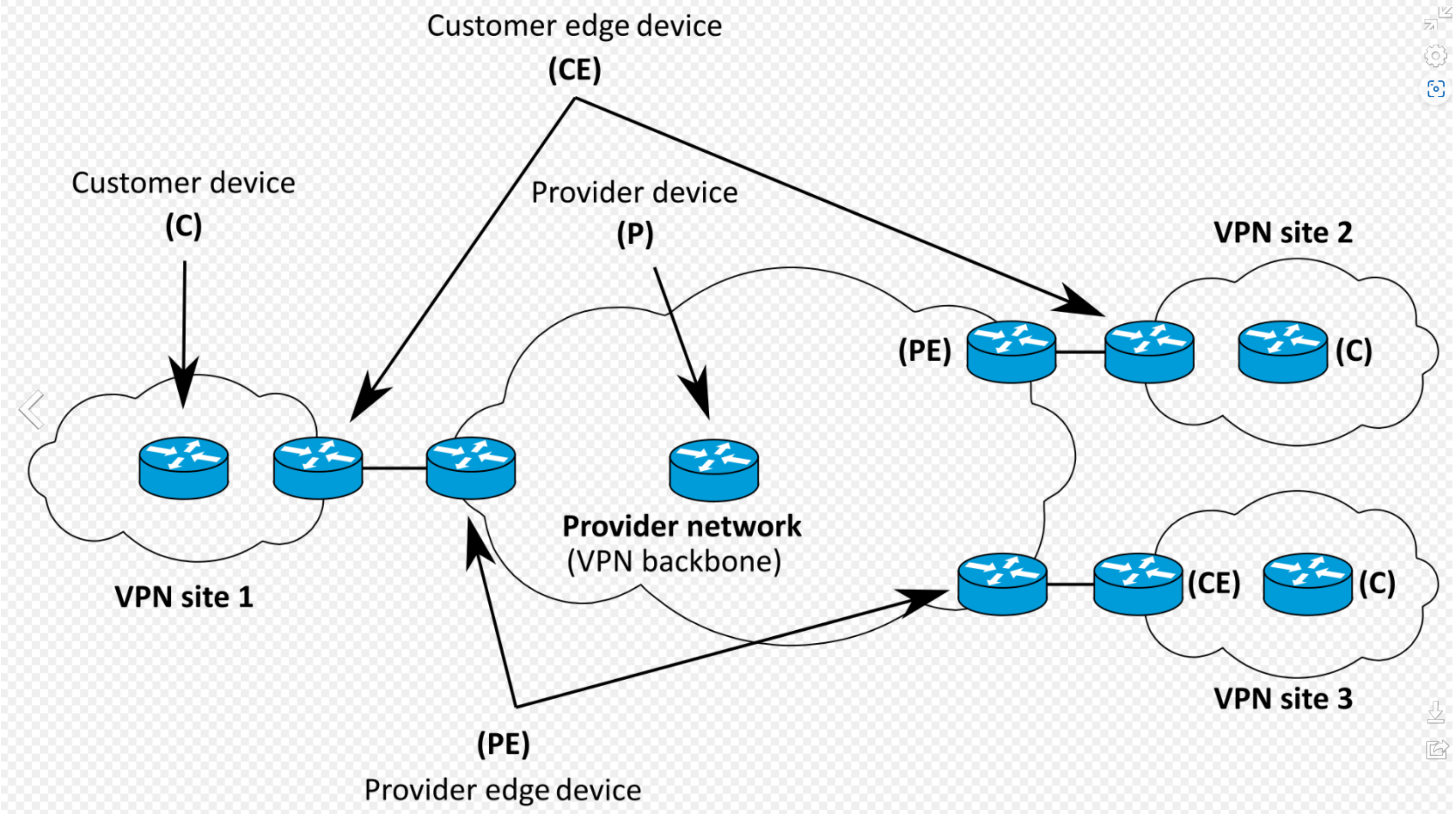
What is VPN? How It Works

- VPN stands for **"Virtual Private Network“**
- establishes a protected network connection when using public networks
- VPNs encrypt your internet traffic and disguise your online identity
- The encryption takes place in **real time**
- This makes it more difficult for third parties to track your activities online and steal data
- A VPN is basically a private tunnel onto the internet that ‘hides’ your identity.

Company VPN


Internet VPN
Internet
Regional Office
Regional Office
Head-office
Remote / roaming users

VPN Service

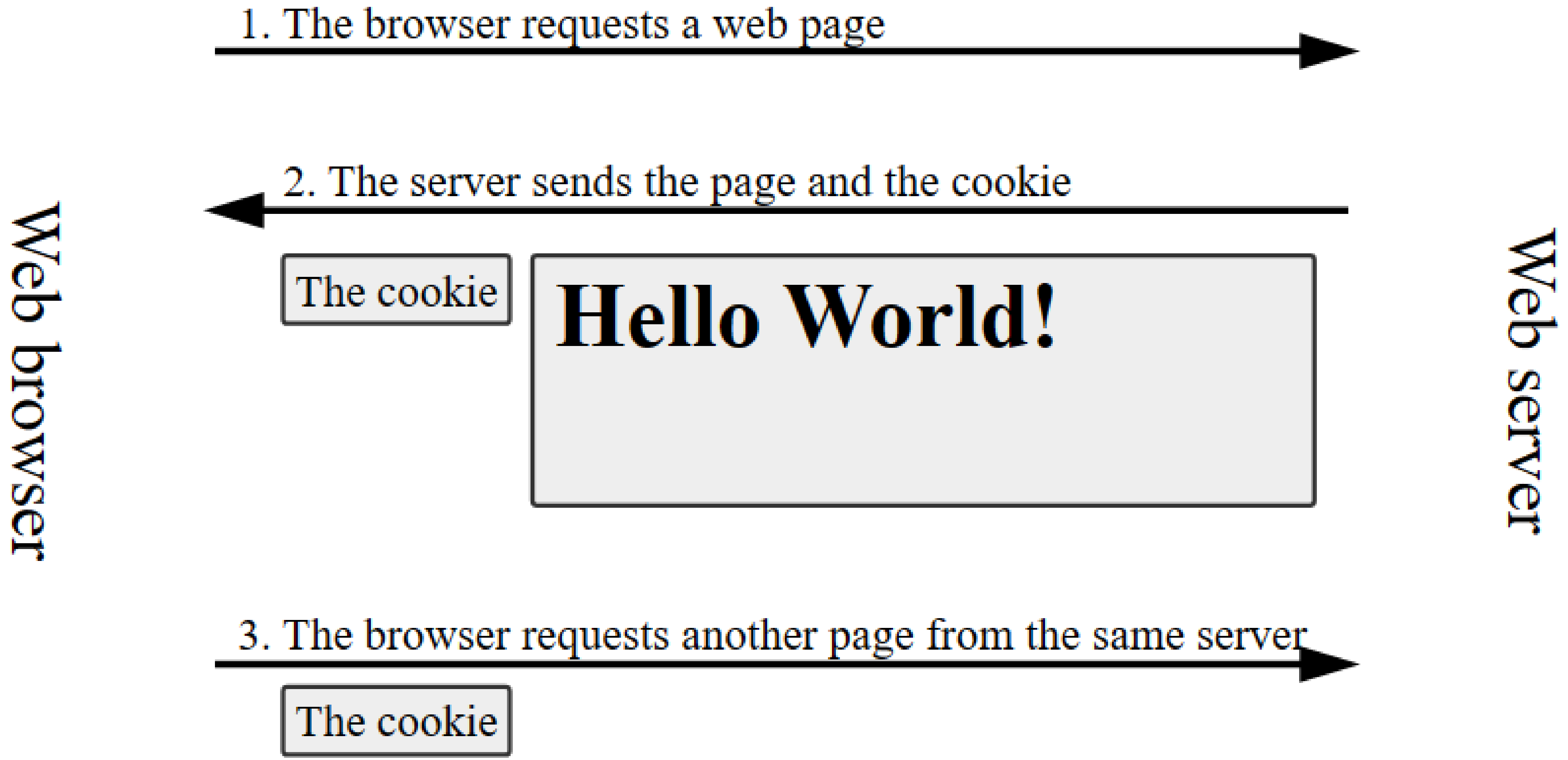

Customer edge device
(CE)
Customer device
(C)
Provider device
(P)
VPN site 2
(PE)
(C)
VPN site 1
Provider network
(VPN backbone)
(CE)
(C)
VPN site 3
(PE)
Provider edge device

Why use a VPN

- Your ISP usually sets up your connection when you connect to the internet. It tracks you via an IP address. Your network traffic is routed through your ISP's servers, which can log and display everything you do online.
- Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.
- This is especially important if you regularly connect to public Wi-Fi networks. You never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity.
- Watch this video

Cookies – why?

- An HTTP cookie stores information in a user's web browser. Web servers generate cookies and send them to browsers, which then include the cookies in future HTTP requests.
- While most cookies are perfectly safe, some can be used to track you without your consent. Worse, legitimate cookies can sometimes be spied upon if a criminal gets access.
- **Cookies** are text files with small pieces of data — like a username and password.
- Data stored in a cookie is created by the server upon your connection. This data is labeled with an ID unique to you and your computer.



Web browser

1. The browser requests a web page

2. The server sends the page and the cookie

The cookie

Hello World!

3. The browser requests another page from the same server

The cookie

Web server

Cookies – how do they work?

- **"Magic cookies"** are an old computing term that refers to packets of information that are sent and received without changes. Commonly, this would be used for a login to computer database systems, such as a business internal network. This concept predates the modern “cookie” we use today.
- **HTTP cookies** are a repurposed version of the “magic cookie” built for internet browsing. Web browser programmer Lou Montulli used the “magic cookie” as inspiration in 1994. He recreated this concept for browsers when he helped an online shopping store fix their overloaded servers.
- The HTTP cookie is what we currently use to manage our online experiences. It is also what some malicious people can use to spy on your online activity and steal your personal info.

- To put it simply, cookies are a bit like getting a ticket for a coat check.
- Here’s how cookie are intended to be used:
    - **Session management.** For example, cookies let websites recognize users and recall their individual login information and preferences, such as sports news versus politics.
    - **Personalization.** Customized advertising is the main way cookies are used to personalize your sessions. You may view certain items or parts of a site, and cookies use this data to help build targeted ads that you might enjoy.
    - **Tracking.** Shopping sites use cookies to track items users previously viewed, allowing the sites to suggest other goods they might like and keep items in shopping carts while they continue shopping.

Why Cookies Can Be Dangerous?

- Since the data in cookies doesn't change, cookies themselves aren't harmful.
- They can't infect computers with viruses or other malware. However, some cyberattacks can hijack cookies and enable access to your browsing sessions.
- The danger lies in their ability to track individuals' browsing histories. To explain, let's discuss what cookies to watch out for.
- **First-party cookies** are directly created by the website you are using. These are generally safer, as long as you are browsing reputable websites or ones that have not been compromised.
- **Third-party cookies** are more troubling. They are generated by websites that are different from the web pages users are currently surfing, usually because they're linked to ads on that page.