


What is an IP Address – Definition and Explanation



We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.



 **Kaspersky
VPN Secure Connection**

**Your browsing is your
business**

Keep your browsing history private with
Kaspersky VPN Secure Connection

[Learn More](#)

What is an IP Address?

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

IP addresses are used to identify devices on a network. They are also used to track your online activity.

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

Watch this video to learn what IP address is, why IP address is important and how to protect it from hackers:



How do IP addresses work

If you want to understand why a particular device is not connecting in the way you would expect or you want to troubleshoot why your network may not be working, it helps understand how IP addresses work.

Internet Protocol works the same way as any other language, by communicating using set guidelines to pass information. All devices find, send, and exchange information with other connected devices using this protocol. By speaking the same language, any computer in any location can talk to one another.

The use of IP addresses typically happens behind the scenes. The process works like this:

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

3. Your IP address is assigned to your device by your ISP.
4. Your internet activity goes through the ISP, and they route it back to you, using your IP address. Since they are giving you access to the internet, it is their role to assign an IP address to your device.
5. However, your IP address can change. For example, turning your modem or router on or off can change it. Or you can contact your ISP, and they can change it for you.
6. When you are out and about – for example, traveling – and you take your device with you, your home IP address does not come with you. This is because you will be using another network (Wi-Fi at a hotel, airport, or coffee shop, etc.) to access the internet and will be using a different (and temporary) IP address, assigned to you by the ISP of the hotel, airport or coffee shop.

As the process implies, there are different types of IP addresses, which we explore below.

Types of IP addresses

There are different categories of IP addresses, and within each category, different types.

Consumer IP addresses

Every individual or business with an internet service plan will have two types of IP addresses: their private IP addresses and their public IP address. The terms public and private relate to the network location — that is, a private IP address is used inside a network, while a public one is used outside a network.

Private IP addresses

Every device that connects to your internet network has a private IP address. This includes computers, smartphones, and

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

IP address, they are also included within the main IP address for your network. As described above, your public IP address is provided to your router by your ISP. Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.

Public IP addresses

Public IP addresses come in two forms – dynamic and static.

Dynamic IP addresses

Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers. Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers. The rationale for this approach is to generate cost savings for the ISP. Automating the regular movement of IP addresses means they don't have to carry out specific actions to re-establish a customer's IP address if they move home, for example. There are security benefits, too, because a changing IP address makes it harder for criminals to hack into your network interface.

Static IP addresses

In contrast to dynamic IP addresses, static addresses remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web.

This leads to the next point – which is the two types of website IP addresses.

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

the same server. This tends to be the case for individual websites or SME websites, where traffic volumes are manageable, and the sites themselves are limited in terms of the number of pages, etc. Websites hosted in this way will have shared IP addresses.

Dedicated IP addresses

Some web hosting plans have the option to purchase a dedicated IP address (or addresses). This can make obtaining an SSL certificate easier and allows you to run your own File Transfer Protocol (FTP) server. This makes it easier to share and transfer files with multiple people within an organization and allow anonymous FTP sharing options. A dedicated IP address also allows you to access your website using the IP address alone rather than the domain name — useful if you want to build and test it before registering your domain.

How to look up IP addresses

The simplest way to check your router's public IP address is to search "What is my IP address?" on Google. Google will show you the answer at the top of the page.

Other websites will show you the same information: they can see your public IP address because, by visiting the site, your router has made a request and therefore revealed the information. The site [IPLocation](#) goes further by showing the name of your ISP and your city.

Generally, you will only receive an approximation of location using this technique — where the provider is, but not the actual device location. If you are doing this, remember to log out of your VPN too. Obtaining the actual physical location address for the public IP address usually requires a search warrant to be submitted to the ISP.

Finding your private IP address varies by platform:

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

On a Mac:

- Go to System Preferences
- Select network – and the information should be visible.

On an iPhone:

- Go to Settings
- Select Wi-Fi and click the "i" in a circle () next to the network you are on – the IP address should be visible under the DHCP tab.

If you need to check the IP addresses of other devices on your network, go into the router. How you access the router depends on the brand and the software it uses. Generally, you should be able to type the router's gateway IP address into a web browser on the same network to access it. From there, you will need to navigate to something like "attached devices," which should display a list of all the devices currently or recently attached to the network – including their IP addresses.

IP address security threats

Cybercriminals can use various techniques to obtain your IP address. Two of the most common are social engineering and online stalking.

Attackers can use social engineering to deceive you into revealing your IP address. For example, they can find you through Skype or a similar instant messaging application, which uses IP addresses to communicate. If you chat with strangers using these apps, it is important to note that they can see your IP address. Attackers can use a Skype Resolver tool, where they

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

Once they have your IP address, attackers can go to an IP address tracking website, such as whatismyipaddress.com, type it in, and then get an idea of your location. They can then cross-reference other open-source data if they want to validate whether the IP address is associated with you specifically. They can then use LinkedIn, Facebook, or other social networks that show where you live, and then see if that matches the area given.

If a Facebook stalker uses a [phishing](#) attack against people with your name to install spying [malware](#), the IP address associated with your system would likely confirm your identity to the stalker.

If cybercriminals know your IP address, they can launch attacks against you or even impersonate you. It is important to be aware of the risks and how to mitigate them. Risks include:

Downloading illegal content using your IP address

Hackers are known to use hacked IP addresses to download illegal content and anything else they do not want to be traced back to them. For example, using the identity of your IP address, criminals could download pirated movies, music, and video – which would breach your ISP's terms of use – and much more seriously, content related to terrorism or child pornography. This could mean that you – through no fault of your own – could attract the attention of law enforcement.

Tracking down your location

If they know your IP address, hackers can use geolocation technology to identify your region, city, and state. They only need to do a little more digging on social media to identify your home and potentially burgle it when they know you are away.

Directly attacking your network

Criminals can directly target your network and launch a variety of assaults. One of the most popular is a [DDoS attac](#)

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

Hacking into your device

The internet uses ports as well as your IP address to connect. There are thousands of ports for every IP address, and a hacker who knows your IP can try those ports to attempt to force a connection. For example, they could take over your phone and steal your information. If a criminal does obtain access to your device, they could install malware on it.



We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

Hiding your IP address is a way to protect your personal information and online identity. The two primary ways to hide your IP address are:

1. Using a proxy server
2. Using a virtual private network (VPN)

A proxy server is an intermediary server through which your traffic is routed:

- The internet servers you visit see only the IP address of that proxy server and not your IP address.
- When those servers send information back to you, it goes to the proxy server, which then routes it to you.

A drawback of proxy servers is that some of the services can spy on you — so you need to trust it. Depending on which one you use, they can also insert ads into your browser.

VPN offers a better solution:

- When you connect your computer – or smartphone or tablet – to a VPN, the device acts as if it is on the same local network as the VPN.
- All your network traffic is sent over a secure connection to the VPN.
- Because your computer behaves as if it is on the network, you can securely access local network resources even when you are in another country.
- You can also use the internet as if you were present at the VPN's location, which has benefits if you are using public Wi-Fi or want to access geo-blocked websites.

Kaspersky Secure Connection is a VPN that protects you on public Wi-Fi, keeps your communications private, and ensures

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

When using public Wi-Fi

When using a [public Wi-Fi network](#), even one that is password-protected, a VPN is advisable. If a hacker is on the same Wi-Fi network, it is easy for them to snoop on your data. The basic security that the average public Wi-Fi network employs does not provide robust protection from other users on the same network.

Using a VPN will add an extra layer of security to your data, ensuring you bypass the public Wi-Fi's ISP and encrypting all your communication.

When you are traveling

If you are traveling to a foreign country – for example, China, where sites like Facebook are blocked – a VPN can help you access services that may not be available in that country.

The VPN will often allow you to use streaming services that you paid for and have access to in your home country, but they are not available in another because of international rights issues. Using a VPN can enable you to use the service as if you were at home. Travelers may also be able to find cheaper airfare when using a VPN, as prices can vary from region to region.

When you are working remotely

This is especially relevant in the post-COVID world, where many [people are working remotely](#). Often employers require the use of a VPN to access company services remotely for security reasons. A VPN that connects to your office's server can give you access to internal company networks and resources when you are not in the office. It can do the same for your home network while you are out and about.

When you just want some privacy

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

services are turned off. Using a VPN prevents you from leaving footprints on the web.

Don't forget your mobile devices, either. They have IP addresses too, and you probably use them in a wider variety of locations than your home computer, including public Wi-Fi hotspots. [It is advisable to use a VPN on your mobile](#) when connecting to a network you may not fully trust.

Other ways to protect your privacy

Change privacy settings on instant messaging applications

Apps installed on your device are a major source of IP address hacking. Instant messaging and other calling apps can be used as a tool by cybercriminals. Using IM apps only allows direct connections from contacts and doesn't accept calls or messages from people you don't know. Changing your privacy settings makes it harder to find your IP address because people who don't know you cannot connect with you.

Create unique passwords

Your device password is the only barrier that can restrict people from accessing your device. Some people prefer to stick to their devices' default passwords, which makes them vulnerable to attack. Like all your accounts, your device needs to have a unique and strong password that is not easy to decode. A strong password contains a mix of upper- and lower-case letters, numerals, and characters. This will help to safeguard your device against IP address hacking.

Stay alert to phishing emails and malicious content

A high proportion of malware and device tracking software is installed via phishing emails. When you connect with any site, this provides the site with access to your IP address and device location, making it vulnerable to hacking. Be vigilant when opening emails from unknown senders and avoid clicking on links that could send you to unauthorized sites. Pay close attention to the emails' content, even if they appear to come from well-known sites and legitimate businesses.

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

the data you send and receive online with VPN.

Protecting your IP address is a crucial aspect of protecting your online identity. Securing it through these steps is a way to stay safe against the wide variety of cybercriminals' attacks.

Related articles:

- [How safe are smart homes](#)
- [Internet of Things security threats](#)
- [What is IP spoofing and how to prevent it](#)
- [What is Voice Over IP \(VOIP\)](#)
- [Tips to protect yourself from cyberstalkers](#)

Featured Articles

[What is DNS hijacking?](#)

[What is an SSID?](#)

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

What is browser isolation and how does it work?

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.



We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

[Kaspersky Standard](#)

[Kaspersky Plus](#)

[Kaspersky Premium](#)

[All Solutions](#)

Small Business Products

(1-100 EMPLOYEES)

[Kaspersky Small Office Security](#)

[Kaspersky Endpoint Security Cloud](#)

[All Products](#)

Medium Business Products

(101-999 EMPLOYEES)

[Kaspersky Endpoint Security Cloud](#)

[Kaspersky Endpoint Security for Business Select](#)

[Kaspersky Endpoint Security for Business Advanced](#)

[All Products](#)



Enterprise Solutions

(1000+ EMPLOYEES)

[Cybersecurity Services](#)

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

© 2023 AO Kaspersky Lab
[Privacy Policy](#) • [Online Tracking Opt-Out Guide](#) • [Anti-Corruption Policy](#) • [License Agreement B2C](#) •
[License Agreement B2B](#)

 Global 

- [Contact Us](#) • [About Us](#) • [Partners](#) • [Blog](#) • [Resource Center](#) • [Press Releases](#)
- [Sitemap](#) • [Careers](#)

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.