IP Masking: What It Is, How It Works, and the Benefits

In an age when billions of private records can be exposed, IP masking is critical for safeguarding online identity. Without it, your digital footprint can lead to invasions of privacy.

This blog post explains the layers of IP masking, how it functions, and the benefits of shielding against unwarranted tracking, profiling, and surveillance.

What is IP masking?

IP masking substitutes a pseudo internet protocol (IP) address instead of the user's IP address. It conceals the user's original address or network device using a proxy server, virtual private network (VPN), or The Onion Router (Tor).

IP masking increases privacy and security by preventing unauthorized tracking or access to the user's physical address and online activities. It can also defeat geo-restrictions and censorship by making the user's traffic appear to be from a different location.

IP masking vs. IP anonymization

While IP masking and IP anonymization may sound synonymous, they're two distinct actions.

IP masking disguises the user's IP identifier to make it seem like their web traffic comes from a different IP address. For example, a website visitor in New Jersey could use a VPN to mask their IP address so that their web traffic appears to be coming from Ireland instead.

IP anonymization alters the user's real IP address by zeroing out the ending or using a substitute. For example, 192.168.1.25 might become 192.168.1.0. This alteration prevents the association of historical or logged data with a specific user, device, or person.

Is it illegal to mask your IP address?

In the United States, masking your private IP address is not illegal. Many businesses and individuals use VPNs for legitimate purposes, such as securing their data while using public Wi-Fi networks.

However, you may need to consult an attorney about state-specific regulations or the General Data Protection Regulation (GDPR) in Europe.

Why do people mask their IP?

While the media commonly portrays criminals using IP masking to conceal fraudulent activities, IP masking actually has many legitimate uses. Here are some of the positive benefits.

Enhanced online privacy and anonymity

With an estimated 3 billion spam messages sent daily, many people worry that their personal information will create a tempting path for sellers, marketers, and cybercriminals:

- **Sellers** collect data to target specific types of people likely to buy their products and services.
- **Marketers** identify returning website visitors to guide them into their sales funnel.
- **Cybercriminals** collect identity data to find and attack those who are vulnerable.

IP masking makes associating your online activity with your IP address is more difficult. Your online footprints don't lead back to you or your device. Instead, they blend harmlessly into the sea of online data.

Protection against tracking and profiling

Many websites and advertisers identify user IP addresses to track data such as sites visited, time spent on pages, and links clicked. They personalize ads based on user profiles that reveal preferences, habits, interests, and demographics.

While personalized ads may be convenient, they may sometimes feel intrusive or manipulative. In the wrong hands, detailed user profiles can enable discriminatory pricing, predatory lending, or ad fraud.

Many people simply feel uncomfortable with the idea of being monitored and profiled.

IP masking disrupts the tracking mechanism. Websites and advertisers see the IP address of the intermediary server (like a VPN server) instead of the user's actual IP, reflecting the *server's* location — not the user's.

Some IP masking solutions use shared IP addresses, where multiple users have the same visible IP. As a result, the data collected is less reliable and, therefore, less valuable for profiling.

Access to geo-restricted content

Media companies often use geo-restrictions to manage digital rights. For example, a streaming service like Netflix might offer different shows in the U.S. than in Germany. With IP masking, a user in Germany could access the American Netflix library with a masked IP address from the United States.

Similarly, IP masking enables sports fans to watch live events restricted in their country due to broadcasting rights.

Accessing geo-restricted content through IP masking allows users to access a broader range of media and services. In regions with internet censorship, IP masking provides access to blocked websites and platforms, enabling freedom of information.

For travelers and expatriates, IP masking helps them stay connected to local news, entertainment, and financial services otherwise inaccessible.

Global content accessibility promotes cultural exchange and global awareness. Accessibility also supports the ideal of a borderless Internet.

Secure online transactions

Secure online transactions form the backbone of e-commerce and financial activities, safeguarding customers' sensitive data to foster digital marketplace confidence. IP masking provides a layer of anonymity over transactions to

defend against cyber-attacks such as phishing or man-in-the-middle schemes that intercept and misuse data.

IP masking dilutes the digital footprint, complicating a cybercriminal's efforts to track and profile user habits and target their financial dealings. This strategic move makes it more difficult for potential attackers to correlate online activities with specific individuals, reducing vulnerability to targeted threats.

IP masking often pairs well with encryption, particularly within VPN services. While IP masking cloaks the user's identity, encryption ensures that any data captured during transit remains encrypted and unintelligible. Encryption keeps the information secure and unreadable in the event of data interception.

Reduced risk of cyberattacks

IP masking defends against cyberattacks such as attacks or targeted hacking attempts.

In distributed denial-of-service (DDoS) attacks, multiple compromised computer systems attack a single target and direct a traffic flood to overwhelm the system. Kaspersky Lab reports that 20% of companies with 50 employees or more reported being victims of at least one DDoS attack.

In targeted hacking, the attacker uses the IP address to gather information, including location, internet service provider (ISP), and network vulnerabilities. IP address masking removes crucial intelligence hackers could exploit.

Moreover, IP masking often involves routing internet traffic through one or several intermediary servers, which hides the user's real IP address and encrypts the data in transit. Even if a hacker intercepts the traffic, the encrypted data and hidden traffic origin provide a dual layer of protection.

Tools and services for IP masking

IP masking tools and services typically fall into one of the following categories:

VPN

A virtual private network (VPN) encrypts the user's internet traffic and routes it through VPN servers worldwide. This process secures the data in transit

from eavesdropping or interception by replacing the user's IP address with one from the VPN server.

VPN encryption keeps data secure, making it ideal for anonymity and protecting information — particularly over unsecured Wi-Fi network connections. This level of security is beneficial for activities such as accessing restricted websites, preventing tracking from advertisers, and safeguarding personal and professional communications.

VPNs come with certain limitations. The encryption process and traffic rerouting through distant servers can result in slower internet speeds as the data travels farther and undergoes complex encryption algorithms.

Additionally, the level of anonymity and security depends on the trustworthiness of the VPN service provider. Since all traffic routes through their servers, a VPN provider could monitor, log, or provide user data to third parties.

Therefore, it's crucial to select a reputable VPN provider with a strict no-logs policy and a proven track record of safeguarding user privacy.

Tor browser

Tor browser (The Onion Router) directs internet traffic through a worldwide network of relay nodes. This intricate design of layered node relays is like the layers of an onion: Each "hop" through relay nodes encrypts and re-encrypts the traffic, making it difficult to trace the connection back to the original user.

Tor's strength lies in its ability to provide anonymity. It’s an essential resource for journalists, activists, and individuals in oppressive regimes where internet use is monitored and censored.

However, Tor’s sophistication comes at the cost of browsing speed — which is slower than a web browser such as Firefox or Chrome. As traffic passes through various relays, latency increases and slows the search engine browsing experience — a byproduct of security measures.

Using Tor can also draw attention, and the entry and exit nodes in the network become theoretically vulnerable to traffic analysis by adversaries. Nevertheless, Tor is a powerful tool for those prioritizing anonymity over speed.

Proxy server

Proxy servers are intermediaries between a user's device and the Internet. The user's internet requests go to the proxy, which forwards the request to the destination website. As a result, the website sees a different IP address provided by the proxy server instead of the user's unique IP address.

Proxy servers can conceal a user's physical location, prevent targeted ads, and allow access to geo-restricted content. This feature can help the user access region-specific marketing data, perform competitor research without revealing one's IP, or bypass censorship in restrictive countries.

Residential proxy servers are a specific type of proxy that uses IP addresses assigned to real residential addresses. The proxy servers appear as legitimate user traffic rather than traffic coming through a data center.

Proxy servers come with limitations. Unlike VPN services, many proxy servers don’t encrypt the connection between the user's device and the proxy, which can leave data vulnerable to interception. Additionally, users must use caution, as unreliable proxy servers can be insecure or log user activity. It’s crucial to select a trustworthy proxy service provider that maintains a strict no-logs policy to ensure privacy and security.

Dynamic IP addresses

Dynamic IP addresses are assigned to devices on a network by an internet service provider (ISP) and can change every time the device connects to the Internet. This fluidity contributes to IP masking by not allowing a single, static point of identification, making it challenging to track user activities or pinpoint their physical location.

Dynamic IP allocation from ISPs has one distinct advantage: efficient reuse of a limited pool of IP addresses among multiple customers. Dynamic IP addresses also require less user maintenance, as IP setting reconfiguration is optional when moving between networks.

However, dynamic IP addresses trace back to the ISP and, subsequently, the user since ISPs log customer data and IP allocations. Furthermore, a dynamic IP address may change during sessions, which can inconveniently interrupt browsing activities. For total anonymity, additional IP masking methods, such as VPNs, proxies, or Tor, are often required.

Nodify and the IPC database with Digital Element

Nodify by Digital Element offers an advanced threat intelligence solution that enhances IP services by providing granular insights into traffic associated with VPNs, proxies, malware, and darknet connections.

Unlike standard cyber threat detection tools, Nodify respects privacy, steering clear of monitoring user or company traffic, and instead furnishes detailed context for each IP address encountered. This protocol allows businesses to decide whether to block or permit specific traffic flows.

Nodify's rich data set includes VPN classifications, provider details such as name and URL, and a clear distinction between residential and commercial IP addresses. These empower users with a deeper understanding of the nature of their traffic.

Nodify maintains a frequently updated database accessible via a RESTful API. It ensures the information on VPNs and proxies is current, refreshing it hourly to maintain robust network security.

Keep your digital presence secure with Digital Element

The ability to discern genuine digital interactions from those cloaked in deception isn't just an advantage — it's a necessity.

Digital Element's Nodify empowers teams to precisely identify and flag IP addresses with a high risk of being masked, enabling a proactive stance against potential threats. By integrating Nodify into their digital security arsenal, businesses can sharpen their edge in risk mitigation and foster a safer online environment.

For those seeking to reinforce their cybersecurity framework and gain the upper hand in the digital landscape, the solution is clear.

Discover how Digital Element's Nodify can fortify your defenses. Visit Digital Element to create a more secure future today.
