Click to prove
you're human

Unblock web browser

Our free Web proxy allows you to unblock any blocked website. Just type the website address in the box and access any site you want. Download Free VPN Free Proxy VPN vs. Proxy comparison Hide.me SOCKS Proxy Get our 5 star VPN app to enjoy gigabit speeds and bulletproof online protection in an easy-to-use package. Download the app We handpick servers that live up to our high standards of security and privacy. They're access controlled, and we are the only ones that operate them — no one else. They do not store IP addresses, nor do they store logs. Each server supports all popular protocols, including: IKEv2, WireGuard, OpenVPN, SoftEther, SSTP and SOCKS. With the very best server locations and low ping times, the internet is yours for the taking — wherever you might be. Beginners, geeks, youngsters, adults... lots of different people from around the world use hide.me everyday. Why? Because it’s safe, simple to use, and supports lots of different devices – from Windows, Mac to Smartphones and even Apple TVs! Our VPN and proxy is supported by all BitTorrent clients, so you don’t have to be a rocket scientist to get up and running with hide.me. Use one of our helpful guides to set up your device and get protected in a few minutes. hide.me VPN proxy is an intermediate server between you and the website you want to browse. A proxy fetches the website and makes it accessible to you. Our free proxy doesn't offer additional encryption but sends your traffic through our web proxy. Just type the website address in the box and access any site you want. For additional protection check our pricing plans. Our proxy doesn't block access to any site, and if you're experiencing trouble accessing a certain page, please contact their owner to check if they're blocking our IP addresses. Our proxy is fast, but does not have the same security as a VPN does. That means your data is not encrypted and should only be used to access blocked websites. Keep this in mind when using our proxy. If you want complete protection, please check our pricing plans. Yes. hide.me VPN proxy is free and requires no installation. On our website you just type the address and access any site unrestricted. As according to our zero log policy, proxy doesn't store any of your data so your private information is safe. A proxy hides only your IP address it doesn't encrypt your web activity. A VPN provides additional protection by encrypting your traffic thus keeping you safe from more sophisticated attacks. hide.me VPN doesn't store any activity logs meaning your internet browsing stays your own. Finland, Germany, and The Netherlands are all available through the hide.me VPN Proxy. Our full VPN service allows you to choose from many more servers. BlockAway is an advanced proxy service that allows you to access any website and safeguard your privacy. It's a free service available to everyone, designed for easy use at school, university, or work without much effort. Enter the address you want and access the internet without any limitations. Hide yourself with BlockAway! BlockAway is a free proxy service that lets you access any website and keep your personal information anonymous. It overcomes various network restrictions, allowing you to watch YouTube videos and use social networks. Our goal is to make information more accessible for everyone. Why you need a proxy server A proxy service acts as a mediator between your device and the Internet. It's straightforward to use – just enter the web address you want to visit. Your request passes through the proxy to the website, and the web content will return to you through the same proxy. This is beneficial if you want to: Hide your network identity. Keep your browsing history private. Open inaccessible websites. However, it's crucial to choose a reliable proxy service. Many on the internet are extremely slow, may disrupt websites and lack video streaming support. BlockAway eliminates these limitations. It's a free and highly advanced proxy solution that can replace other web proxies or VPN services. What makes a good proxy browser? When selecting the best proxy browser, consider the following criteria: High-speed data transfer. Anonymity and the ability to visit blocked websites. Support for different types of websites without breaking or modifying content. Additional advantages, such as faster processing due to proper caching and data compression. This is a basic list of essential features to help you make the right proxy browser choice. Of course, you can also opt for a VPN service as an alternative to a proxy site. However, many VPN services are paid and designed for professional usage. In comparison, BlockAway is free and doesn't require any configuration. Key features of the web proxy BlockAway provides everything you need for a safe and secure internet presence, addressing typical issues associated with proxy services. Key features of the proxy browser include: Advanced technology for compatibility with popular websites. High security and privacy. Unlimited video access on YouTube and other video websites and social networks. Europe and USA proxy server options for connection. No browser or operating system configuration required. Ability to share a proxy link with friends. The basic version is free of charge. One of the beautiful things about the internet is just how accessible it is. You can be anywhere in the world at any time of the day and still be able to email your friends, find the football results, discover delicious cupcake recipes, and find the best open café in your 200-metre vicinity.But dig beneath the surface and the more you use the internet, the more you realise that there are actually a lot of areas that you can't access. From pure geo-restrictions that mean you have to be in a certain country to view a site, to localised TV broadcasts or sites that countries have flat-out banned, a tool to unblock websites is a useful thing to have on your laptop and phone.That's where using one of the best VPNs comes in. It's affordable, versatile software that has crossed over from being a niche business tool to being widely used across the world to access banned web pages and getting around blocked services. Below we'll explain what they are, how to use them and which ones are best to help you unblock websites with ease. You may like Today's best 3 VPNs to unblock websitesHow does a VPN help to unblock websites?Virtual private networks work by channelling all of the internet traffic you receive through a secure VPN server. And they work whether that traffic flows through your computer, TV, streaming device, games console, or your phone using a mobile VPN app. Not only does this make your internet use really secure - everything is strongly encrypted - but it also means you can effectively spoof the IP address of your device. Simply put, that means you can appear like you're in completely different zip code, city or country to the one you're actually in.So if, for example, you're physically in China where loads of online services like Google, YouTube, Facebook, WhatsApp and many more are banned, you can use VPNs for China to virtually relocate yourself to a country where they're not.The same method applies if, say, your school or office has cut access to social media and video sites. And this even extends to more far-reaching uses like watching Netflix content or live sports that are only available in other regions.Sign up to the TechRadar Pro newsletter to get all the top news, opinion, features and guidance your business needs to succeed!How to change location with a VPN and unblock websitesBelieve it or not, it's really very straightforward to change location and IP address with a VPN:Find and download a reliable VPN – or simply head straight to ExpressVPNInstall it on to your computer, mobile or other chosen deviceOnce everything is ready, open the VPN applicationLog-in with your details, follow any welcome prompts, and you should soon be offered a list of VPNs to connect toPick the country you want your computer to change to (so somewhere that the site is not blocked) and click the appropriate buttonHead to the blocked site. As your device now thinks it's somewhere that the service is allowed, you'll now discover that it is an unblocked website(Image credit: PK Studio / Shutterstock.com)Unblock websites: which sites and services can I unlock?The short answer here is: pretty much any. In our experience, the best VPN providers out there have a very impressive hit rates when it comes to how they unblock websites.Below is a far from exhaustive list of websites that are banned around the world or carry geo-restrictions.When it comes to TV, films and sport, it's certainly a very common practice that coverage is blocked to specific regions - little wonder that Netflix VPNs and streaming VPNs have grown in popularity in recent years.. But some of the more surprising additions to the list are the kind of sites that the most censor-happy countries in the world ban or have banned.Amazon Prime VideoBBCBBC iPlayerCNNFacebook (and Messenger)GmailGoogle Apps (e.g. Calendar, Docs, Hangouts, Maps, etc)HootsuiteHuluInstagramOneDriveNetflixNew York TimesPinterestRedditReutersSlackSnapchatSling TVSpotifyTwitchTwitterWall Street JournalWikipediaWhatsAppYouTubeWhere am I most likely to want to unblock websites?As we say, governments in some countries are less fond of internet freedoms than others. It's no great surprise that people using VPNs for China has grown massively, as its Communist ruling party have put bans in place on pretty much every site on the above list.But China isn't alone in this, and if you're visiting any of the following countries any time soon, then we'd advise you to grab a VPN before you go:- Best UAE/Dubai VPN- Best Turkey VPN- Best India VPN- Best Cuba VPNRather a lot - they are really versatile pieces of kit and there are many VPN uses availableTheir primary function really is as an extra layer of security for your online life. When turned on, all of your internet activity is encrypted and you're effectively completely anonymous. So if you don't like the idea of being tracked online, then they're probably a better fit than more traditional antivirus software. We think they're especially useful when you use public, insecure Wi-Fi.It's a similar theme if you're somebody who uses a VPN for torrenting. A virtual private network is an essential piece of kit these days to ensure that your internet service provider - or anybody else for that matter - can't see if or what you're torrenting.Some uses are a bit more niche. More and more people turn their VPNs on when shopping for flights and such. By not giving the site any clues as to your true IP address, you circumvent any targeted price increases.Keeping VPNs on the DL While a VPN remains an excellent way to unblock sites, bad actors like rogue governments know this too and take steps to try to restrict VPN use or block it altogether.This is where obfuscation technology comes in. This works by giving you all the privacy benefits of a VPN but tries to disguise your traffic so those with access to your connection records will find it very difficult to detect you’re connected to a VPN in the first place.If you’re worried about others using a VPN, you’ll be pleased to know that major providers have heard you. ProtonVPN is one of the many services that has developed its very own stealth protocol, which is designed to make your VPN traffic look like regular HTTPS. VyprVPN also has developed the “Chameleon Protocol”, which not only disguises your traffic but uses “Smart IP” to cycle your connection between different servers, making it harder for bad actors to practise DPI (Deep Packet Inspection) of your data. In both cases these protocols are available at no extra charge to users. Keep your SOCKS on Although it’s only good news that VPN providers are taking steps to disguise your traffic, for people living in regimes which restrict or ban VPNs these may not be an option. The websites to download the VPN client themselves might be blocked. Users in less economically developed countries might also be unable to afford VPN subscription fees.Free VPNs are also problematic, as it’s hard to trust they aren’t selling your data in order to keep the lights on. We’ve reviewed some of the best free VPN providers this year but use them at your own risk. This is where SOCKS5 can be useful. It's a much more secure version of the SOCKS protocol, which allows you to connect more securely to a proxy server.You can read more about the differences between a proxy and VPNs in our guide but for now it’s enough to know that when you connect to a SOCKS5 proxy, your IP address is disguised from the Internet in general. If the proxy server is located in another country, this is a great way to evade censorship, as you can access online services like the Wall Street Journal even if they’re banned in your home country.This is usually a lot faster and cheaper to set up than a VPN, although it comes at a price. The SOCKS5 protocol doesn’t have any built-in way to encrypt your data, so anyone would access to your connection records could detect what you’ve been up to.Mindful of this, Chinese developer codename “clowwindy” created the free and open source “Shadowsocks” protocol in 2012. It encrypts connections over SOCKS5 proxies as well as disguising your data to appear like regular SSL/TLS traffic. As this type of data is so common this makes it very difficult to detect that you’re concealing any data in the first place. This may have been the reason that the Chinese government “asked” clowwindy to remove the Shadowsocks code from Github in 2015, though others have carried on his work. Whilst Shadowsocks remains very easy to set up and provides an excellent way to disguise your traffic, you have to configure each application you want to use with it e.g. your web browser and P2P software. VPNs on the other hand will connect securely to a server and protect all your traffic by default, so are a better choice for keeping your data safe. Onto Tor If you want to access restricted content quickly, easily and free of charge you can do worse than use Tor. This establishes an encrypted connection over a number of servers or ‘relays’ within its network. This conceals your IP address and encrypts your traffic, so it’s virtually impossible for anyone connected to the Tor network to know where you are or what you’re accessing.Volunteers around the world also run ‘exit nodes’ which you can use to access the regular internet. As these are based in other countries you can usually access content such as Instagram in the same way as anyone else in that country.Tor data packets are quite distinctive, so some countries like China have made efforts to block people using the software. You can reduce the chance of this happening by using a Tor Bridge. These are run by volunteers and help you connect to the Tor network without revealing to your ISP that you’re doing so. (Image credit: Tor)If you do use the Tor Browser, remember that anonymity comes at a price. Routing data through multiple servers can seriously slow down your connection. Some exit nodes are also run by bad actors who’ll try to harvest your personal information.You can avoid this problem altogether by using only Tor ‘hidden services’, which use the .onion suffix. Many western news outlets can be accessed this way by the dark web such as BBC News (and the New York Times ( )If you have to access the regular internet via Tor exit nodes, you can also stay safe by encrypting your traffic. This can be as simple as using sites that support SSL and TLS (look for the padlock icon in your address bar). Some VPN providers also host “Onion over VPN” servers, so you can use the Tor network whilst encrypting your traffic via a VPN. This not only shields the fact you’re using Tor but hides your IP address when you first connect to the dark net.Unblocking overall There are various ways to unblock restricted websites and apps around the world. Which one is best is entirely a matter for you. VPNs offer some powerful privacy features but some websites and governments try to block them. Proxy servers like those used via Shadowsocks make your activity almost impossible to detect but don't do much to encrypt it. Tor will both encrypt your traffic and conceal your location but can be very slow, plus you need to be careful about ‘poisoned’ exit nodes. Make sure to thoroughly research whatever provider you use so you fully understand pros and cons. Best business VPNs: Keep employees secure when connected These step-by-step tutorials will show you how to unblock blocked websites in several ways using tricks, free software, online services, DNS, and apps. Blocked websites When you're bored at your office, school, or home and have some spare time, you might want to go online and visit your favorite site, like Facebook, YouTube, Twitter, Vimeo, Yahoo, Gmail, VK, Reddit, Pinterest, Google, LinkedIn, or another website to check your email, check what your friends are sharing, watch videos, play video games, chat with someone, or do other things online. So you open your web browser and visit your favorite website but then find out that the site is blocked. And: You might get one of the following messages in your web browser: DENIED, ACCESS DENIED, This site can't be reached, Hmm. We're having trouble finding that site. We can't connect to the server at vimeo.com., or Hmmm...can't reach this page. There are schools, companies, and even countries that block certain websites like social media, video sharing, political, news, and adult sites. When it happens only at work or school, it's probably blocked by the company's or school's network administrator. But: There are also countries where governments (authorities) block certain websites. Countries may block websites for the following reasons: Political: Views and information in opposition to those of the current government or related to human rights, freedom of expression, minority rights, and religious movements. Social: Views and information perceived as offensive or as socially sensitive, often related to sexuality, gambling, or illegal drugs and alcohol. Conflict/Security: Views and information related to armed conflicts, border disputes, separatist movements, and militant groups. Internet Services: Email services (e.g., Gmail, Yahoo Mail, Outlook.com, AOL Mail) Search engines (e.g., Google, Bing, Yahoo, DuckDuckGo, Baidu) Translation (e.g., Google Translate, WorldLingo, SDL FreeTranslation, Bing Translator) Voice-over Internet Protocol (VoIP) services (e.g., Skype, Google Hangouts, Vonage) Censorship or filtering circumvention methods Web hosting You can try several methods to unblock websites. Many people use proxy sites, but you can also unblock websites without them. On this page, you'll find a few methods to bypass restrictions and access blocked websites. How to unblock a blocked website using DNS over HTTPS (DoH) DNS over HTTPS is an internet security protocol that improves privacy and security by encrypting your DNS requests. The benefits of this internet security protocol are that encrypting DNS requests helps hide your online activities and ensures that attackers cannot forge or alter DNS traffic. You can also use DNS over HTTPS to try to unblock blocked websites. On this page, you'll find several methods to enable DNS over HTTPS in Windows 11, Google Chrome, Microsoft Edge, and Firefox. How to enable DNS over HTTPS in Windows 11 Right-click on the Windows start menu button. Click on Settings. Click on Network & Internet in the left menu. Click on Wi-Fi or Ethernet (Internet (LAN) cable). This depends on how your PC is connected to the internet. Click on Hardware properties. Click on Edit next to DNS server assignment. Select Manual. Click on the Ipv4 toggle button to turn it on. Enter a primary DNS server address in the Preferred DNS field (e.g., 8.8.8.8 or 1.1.1.1). Select On (automatic template) at DNS over HTTPS. Enter a secondary DNS server address in the Alternative DNS field (e.g., 8.8.4.4 or 1.0.0.1). Select On (automatic template) at DNS over HTTPS. Click on the Ipv6 toggle button to turn it on. Enter a primary DNS server address in the Preferred DNS field (e.g., 2001:4860:4860::8888 or 2606:4700:4700::1111). Select On (automatic template) at DNS over HTTPS. Enter a secondary DNS server address in the Alternative DNS field (e.g., 2001:4860:4860::8844 or 2606:4700:4700::1001). Select On (automatic template) at DNS over HTTPS. Click on Save. DNS over HTTPS is now enabled in Windows 11. Your DNS requests will be private and secure. How to enable DNS over HTTPS in Google Chrome Google Chrome may already have DNS over HTTPS enabled by default. However, it's better to double-check and possibly make changes, such as changing the DNS service provider. Click on the three-dot menu button in the top right corner of Google Chrome. Click on Settings. Click on Privacy and security in the left menu. Click on Security. Click on the Use secure DNS option to turn it on. Select a DNS provider (e.g., Google Public DNS). DNS over HTTPS is now enabled in Google Chrome. You may need to restart your web browser before visiting the blocked website. If the website is still blocked, try using another DNS service provider. How to enable DNS over HTTPS in Microsoft Edge Microsoft Edge may already have DNS over HTTPS enabled by default. However, it's better to double-check and possibly make changes, such as changing the DNS service provider. Click on the three-dot menu button in the top right corner of Microsoft Edge. Click on Settings. Click on Privacy, search, and services in the left menu. Scroll down to the Security section. Click on the Use secure DNS to specify how to lookup the network address for websites option to turn it on. Select the Choose a service provider option. Select a DNS provider (e.g., Google Public DNS). DNS over HTTPS is now enabled in Microsoft Edge. You may need to restart your web browser before visiting the blocked website. If the website is still blocked, try using another DNS service provider. How to enable DNS over HTTPS in Firefox Firefox may already have DNS over HTTPS enabled by default. However, it's better to double-check and possibly make changes, such as changing the DNS service provider. Click on the three-line menu button in the top right corner of Firefox. Click on Settings. Click on Privacy & Security in the left menu. Scroll down to the DNS over HTTPS section. Select the Max Protection option. Select a DNS provider (e.g., Cloudflare). DNS over HTTPS is now enabled. You may need to restart your web browser before visiting the blocked website. If the website is still blocked, try using another DNS service provider. How to unblock a blocked website using a different DNS provider DNS (Domain Name System) lets users connect to websites using domain names instead of IP addresses. DNS is the phonebook of the internet. You can use Google Public DNS or Cloudflare's 1.1.1.1 public DNS resolver to try to unblock blocked websites. Below you will find steps to change DNS settings in Windows 10, Windows 11, and Android. Change DNS settings on Windows 10 Click or right-click on the Windows start menu button. Click on Settings. Click on Network & Internet. Click on Properties below your Internet network. Click on Edit under 'IP settings' and 'IP assignment'. In the 'IP settings' window, you select Manual. Click on the Ipv4 toggle button to turn it on. Enter a primary DNS server address in the Preferred DNS field (e.g., 8.8.8.8 or 1.1.1.1). Enter a secondary DNS server address in the Alternative DNS field (e.g., 8.8.4.4 or 1.0.0.1). Click on Save. Your DNS settings are now changed. Change DNS settings on Windows 11 Right-click on the Windows start menu button. Click on Settings. Click on Network & Internet in the left menu. Click on Wi-Fi or Ethernet (Internet (LAN) cable). This depends on how your PC is connected to the internet. Click on Hardware properties. Click on Edit next to DNS server assignment. Select Manual. Click on the Ipv4 toggle button to turn it on. Enter a primary DNS server address in the Preferred DNS field (e.g., 8.8.8.8 or 1.1.1.1). Select On (automatic template) at DNS over HTTPS. Enter a secondary DNS server address in the Alternative DNS field (e.g., 8.8.4.4 or 1.0.0.1). Select On (automatic template) at DNS over HTTPS. Click on the Ipv6 toggle button to turn it on. Enter a primary DNS server address in the Preferred DNS field (e.g., 2001:4860:4860::8888 or 2606:4700:4700::1111). Select On (automatic template) at DNS over HTTPS. Enter a secondary DNS server address in the Alternative DNS field (e.g., 2001:4860:4860::8844 or 2606:4700:4700::1001). Select On (automatic template) at DNS over HTTPS. Click on Save. DNS over HTTPS is now enabled in Windows 11. Your DNS requests will be private and secure. Change DNS settings on Android Open your phone's settings. Tap on Connections or Network & internet. Tap on Private DNS. If you don't see the 'Private DNS' option, you may have to tap on More connection settings or Advanced. Tap on Private DNS provider hostname to enable this option. Enter dns.google or one.one.one.one (Cloudflare) or 1dot1dot1dot.cloudflare-dns.com or dns.quad9.net or dns.adguard.com in the field below Private DNS provider hostname. You may need to test these DNS providers to see which one works best for you in terms of speed. Tap on Save. Your DNS settings are now changed. If you have an Android phone or tablet with an older version of Android, you can use an app like Cloudflare's 1.1.1.1 app. How to unblock a blocked website using a VPN A VPN (Virtual Private Network) is a technology that encrypts your internet traffic and hides your IP address. You can use a VPN to access region-restricted websites, shield your internet browsing activities on public Wi-Fi networks, and more. There are many paid and free VPN services and applications available for Windows, macOS, Linux, Android, and iOS. Four examples of well-known VPN services are: Most VPNs are easy to use: you open the application, select a region, and click the connect button. Some VPNs, like Windscribe, also offer browser extensions for Google Chrome, Microsoft Edge, and Firefox. How to unblock a blocked website using Tor Browser Tor Browser is a web browser that relays and encrypts your traffic as it passes through the Tor network. This network comprises thousands of volunteer-run servers known as Tor relays. Tor Browser blocks third-party trackers, ads, and fingerprinting, and it allows you to access blocked websites. You can use the Tor browser on Windows, macOS, and Linux without installing it. It can also be run directly from a USB flash drive. You can download the Tor browser from . Simply open the Tor Browser and visit the blocked website. How to unblock a blocked website using Tails Tails is a portable operating system that uses the Tor network to relay and encrypt your internet traffic. You can run Tails from a USB flash drive. Download Tails. Install Tails on a USB flash drive. Shut down your computer. Start your Tails USB flash drive instead of starting on Windows, macOS, or Linux. Open the web browser. Visit the blocked website. How to unblock a blocked website using proxy sites A proxy site is a website hosted on a server that redirects your web browsing activity, acting as an intermediary between you and the website you want to visit. You can use proxy sites to access blocked websites. Note: Some companies, schools, or countries block proxy sites and might regularly update their list of blocked proxy sites. Therefore, it may be useful to maintain a list of proxy sites. How to unblock a blocked website using an IP address Sometimes only the URL of a website is blocked (e.g., www.facebook.com, www.reddit.com, x.com), but you might still be able to visit the site by using its IP address (e.g., 206.189.189.27). Not all websites can be accessed by their IP address. The group of numbers is the IP address of the website (e.g., 185.60.218.35). How to find a website's IP address on Windows, Linux, and macOS In this example, I'll be using Facebook. Open the Windows Terminal or Command Prompt, Linux Terminal, or macOS Terminal. Type the following command: ping facebook.com Press the Enter or Return key on your keyboard. The group of numbers is the IP address of the website (e.g., 185.60.218.35). How to unblock a blocked website using a URL shortener The URL (web address) of the website you want to visit might be blocked, but converting it to a shorter URL with the help of a URL shortener might help you access the blocked site. The URL shortener will now create a custom short URL. You can use this URL to visit the blocked website. Check the Windows Hosts file The Windows Hosts file can also be used to block websites. If a website is blocked, it's a good idea to check the Windows Hosts file as well. Click on the Windows start menu button. Type notepad. Right-click on Notepad when it appears in the search results. Click Run as administrator. If the 'User Account Control' window appears, you click Yes. Depending on your settings, you may also need to enter the admin password and click Yes. Click File located in the top left corner of Notepad. Click Open. Navigate to the following location on your PC: (C:) > Windows > System32 > drivers > etc. Click Text Documents (*.txt) located in the bottom right corner of Notepad. Select All Files (*.*). Select the hosts file. Click Open. If you see the blocked website, the Windows Hosts file blocks it. To unblock it, remove the website from this file. localhost name resolution is handled within DNS itself. 127.0.0.1 www.example.com 127.0.0.1 example.com Click File located in the top left corner of Notepad. Click Save. Close Notepad. Internet Related: How to enable DNS over HTTPS in Windows 11 (step by step) How to use Private DNS on an Android phone or tablet How to set up DNS on any Android phone (step by step) How to access blocked websites on an Android phone without VPN How to block a website in Windows 10 and 11 (step by step) Access any blocked website instantly with our free proxy service. No registration, no installation - just enter URL and browse securely with military-grade encryption.