# How To Circumvent Online Censorship

Many governments, companies, schools, and public access points use software to prevent Internet users from accessing certain websites and Internet services. This is called Internet filtering or blocking and is a form of censorship. Content filtering comes in different forms. Sometimes entire websites are blocked and sometimes content is blocked based on keywords contained in it. One country might block Facebook entirely, or only block particular Facebook group pages?or it might block any page or web search with certain words in it.

Regardless of how content is filtered or blocked, you can almost always get the information you need by using a circumvention tool. Circumvention tools usually work by diverting your web or other traffic through another computer, so that it bypasses the machines conducting the censorship.

There are different ways of circumventing Internet censorship, some of which provide additional layers of security that you may need. The tool that is most appropriate for you depends on your threat model. If you?re not sure what your threat model is, you should work it out using the [Managing Information lesson](umbrella://lesson/managing-information). Users with a high threat model who need to ensure total anonymity online should use tools outlined in the Advanced section of this lesson.

# HTTPS

HTTPS is the secure version of the HTTP protocol used to access websites. Sometimes a censor will block the insecure version of a site only, allowing you to access that site simply by entering the version of the domain that starts with HTTPS. This is particularly useful if the filtering you're experiencing is based on keywords or only blocks individual web pages. HTTPS stops censors from reading your web traffic, so they cannot tell what keywords are being sent, or which individual web page you are visiting (censors can still see the domain names of all websites you visit).

If you suspect this type of simple blocking, try entering https:// before the domain in place of http://.

Try EFF?s [HTTPS Everywhere](https://www.eff.org/https-everywhere) plug-in to automatically turn on HTTPS for those sites that support it.

# Website variations

Another way that you may be able to circumvent basic censorship techniques is by trying an alternate domain name or URL. For example, instead of visiting http://twitter.com, you might visit http://m.twitter.com, the mobile version of the site. Censors that block websites or web pages usually work from a blacklist of banned websites, so anything that is not on that blacklist will get through. They might not know of all the variations of a particular website's domain name?especially if the site knows it is blocked and registers more than one name.

# Web-based proxies

A web-based proxy (such as <https://proxy.org/>) is one of the simplest ways of circumventing censorship. It is a website that lets its users access other, blocked or censored websites. In order to use a web-based proxy, all you need to do is enter the filtered address that you wish to use into the box in the proxy webpage; the proxy will then display the requested content inside its own webpage.

Web-based proxies are a good way to quickly access blocked websites, but they have certain disadvantages, as well.

* They often don?t provide any security and will be a poor choice if your threat model includes someone monitoring your internet connection.
* They do not always display pages correctly, and many web-based proxies will fail to load complex websites, including those that feature streaming audio and video content.
* And, of course, web-based proxies only work for webpages. You cannot, for example, use an instant messaging program or an email client to access blocked services through a web-based proxy.
* Finally, web-based proxies themselves pose a privacy risk for many users, depending on their threat model, since the proxy will have a complete record of everything you do online.

There are numerous proxy tools that use encryption, providing an additional layer of security, as well as the ability to bypass filtering. Although the connection is encrypted, the tool provider may have your personal data, meaning that these tools do not provide anonymity. They are, however, more secure than a plain web-based proxy. The simplest form of an encrypted web proxy is one that starts with ?https??this will use the encryption usually provided by secure websites.

# Virtual Private Networks

A Virtual Private Network (VPN) encrypts and sends all Internet data between your computer and another computer. This computer could belong to a commercial or non-profit VPN service, your company, or a trusted contact. A proxy server is mainly for web traffic only, but a VPN encrypts and protects all traffic. The main difference is that a VPN server encrypts your data, but a proxy server does not. A VPN also lets you use more than just the Internet ? you can use it to access webpages, e-mail, instant messaging, VoIP and any other Internet service.

## Psiphon3

Psiphon3 is a secure, public circumvention tool that combines VPN, SSH and HTTP Proxy technology to provide you with uncensored access to Internet content. It is available free online for Windows and Android. You can learn how to use it in the [Psiphon3 tool guide](umbrella://lesson/psiphon).  
Because Psiphon 3 is VPN-based, it is able to proxy all of your Internet traffic, not just websites. It should be noted that although Psiphon is does not allow individual user?s IP addresses to be associated with any individual website visited, Psiphon is intended primarily as a censorship evasion tool, rather than one that guarantees anonymity.

For information about other VPN services and to figure out which one might be right for you, click [here](http://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/). Do not use a VPN that you do not trust.

While a VPN protects your traffic from being intercepted locally, your VPN provider can still keep logs of what websites you access or even provide a third party with the ability to snoop directly on your web browsing. Depending on your threat model, the possibility of a government listening in on your VPN connection or obtaining the logs may be a significant risk and, for some users, could outweigh the short-term benefits of using a VPN. These users, or anyone who requires total anonymity online, should use Tor, as described in the Advanced section of this lesson.

# Circumventing censorship from your smartphone

Using your smartphone to go online is often risker than using a computer. You can reduce your risks through the use of these tools.

Using a VPN on your mobile will give you uncensored access to Internet content while encrypting what you do. We recommend using the Psiphon3 tool, outlined above, which works on Androids as well as Windows.

Users with a high threat model who need to ensure total anonymity online should use tools outlined in the Advanced section of this lesson.

## Proxies

Using proxies on your mobile phone will allow you to access otherwise blocked websites. You can access proxies by downloading the mobile version of Firefox ? [Firefox mobile](http://f-droid.org/repository/browse/?fdid=org.mozilla.firefox) along with the [Proxy Mobile](https://guardianproject.info/apps/proxymob-firefox-add-on/) add-on which makes proxying with Firefox easy. It is helpful in cases of censorship, but still may reveal your requests unless the connection from your client to the proxy is encrypted. This can be used on Androids as well as iPhones.

## Virtual Private Network (VPN)

Using a VPN on your mobile will give you uncensored access to Internet content while encrypting what you do. We recommend using the [Psiphon3](umbrella://lesson/psiphon) tool, outlined above, which also works on Androids.

Users with a high threat model who need to ensure total anonymity online should use tools outlined in the Advanced section of this lesson.

Swipe right for this lesson's checklist

Go to the Advanced lesson for advice on how to ensure you stay anonymous online.

[Go to Advanced Lesson](umbrella://lesson/the-internet/1)

### RELATED LESSONS/TOOLS

* [Managing Information lesson](umbrella://lesson/managing-information)
* [Psiphon3 tool guide](umbrella://lesson/psiphon)
* [Proxy Mobile tool guide](umbrella://lesson/proxy-mobile)

### FURTHER READING

* [EFF - How to circumvent online censorship](https://ssd.eff.org/en/module/how-circumvent-online-censorship)
* [Floss manuals - Bypassing censorship](en.flossmanuals.net/bypassing-censorship/)
* [OpenNet - Outlining internet restrictions](https://opennet.net)