

# How to use proxies and surf safe

**Source:** <http://www.derkeiler.com/Newsgroups/alt.computer.security/2003-05/0417.html>

---

**From:** Dave ([dave4550\\_at\\_hotmail.com](mailto:dave4550_at_hotmail.com))

**Date:** 05/14/03

Date: 14 May 2003 03:22:34 -0700

First of all, you need to connect through a proxy.

Just like <http://www.megaproxy.com> and <http://www.anonymizer.com> there are thousands of free proxies which allow you connect anonymously and securely to the website of your choosing.

Go to <http://proxysite.com/> and choose a proxy computer in the country of your choice. There are anonymous proxies, and transparent proxies, and you want to choose an anonymous proxy that totally masks your IP from the website (i.e. computer) which you connect to.

Once you've chosen your proxy, open Internet Explorer 5.5 and go to Tools/Internet Options/Connections

If you have cable modem or broadband connection click on "LAN Settings," check "Use a proxy server" and enter the proxy IP number, and port in the boxes.

If you're on a dialup connection go to Tools/Internet Options/Connections

In the white "Dial-up settings" box, highlight the connection you use. Click on "Settings." Check "Use a proxy server" and enter the proxy IP number, and port in the boxes.

Click "Okay."

Once you have your proxy, go to <http://www.all-nettools.com/pr.htm> to check if you are really anonymous.

Connecting to a proxy server is just like connecting to a website. All the internet is, is computers, and a webserver which serves websites, is just another computer. When you connect to the website Yahoo for example, you are immediately proxied through several other computers which handle Yahoo's web traffic. The "web address" is just a mask for a computer's IP number. For instance <http://www.all-nettools.com> is just a domain name for the computer at IP address <http://216.92.207.177>. Connect to <http://216.92.207.177>

and you will see that it is exactly the same website.

To clear your computer of your past surfing content,

Go to Tools/Internet Options/General/

Clear History

Delete Files

Delete Files–Delete Offline Content

Then go to the tab "Content" AutoComplete – Clear Forms, Clear Passwords.

To make sure the websites aren't tracking you, delete all your cookies

Go to Windows Explorer

C:/Windows/Temporary Internet Files/

Edit/"Select All" or Cntrl+A

Delete

C:/Windows/Cookies

Delete

C:/Windows/Temp/Cookies

Delete

To turn off your cookies so that you don't have to delete them as often, in Internet Explorer 5.5 go to Tools/Internet Options/Security "Custom Level," scroll down until you see "Allow cookies that are stored on your computer," select Disable, and click Okay.

If anyone knows anything else to clear, please let me know. Remember, your Internet Service Provider (ISP) could still be watching you, but if you connect through a proxy they would have packet sniff to see what you're looking at. You could get around this with an encrypted proxy such as <http://www.megaproxy.com>, which encrypts your packets so long as whoever is trying to monitor you does not have the de-encryption keys. Also remember that if you post something through a proxy you could still be traced if the proxy computer you connect through keeps logs.

In my opinion, the internet should be 100% anonymous in any case. No one has any authority to look at any of your web communications without a court order, and countries have no authority to regulate communications between people, on the net or otherwise.

Also note that if you're using a proxy, a downloaded Yahoo program such as chat or games, or movies, automatically opens a new program which may NOT connect through the proxy, and could reveal your real IP.

## alt.computer.security: How to use proxies and surf safe

For more information on the internet and to test the safety of your computer, go to <http://www.grc.com> or <http://www.privacy.net>.

It's also a good idea to have a good firewall. Zone Alarm is one of the best, you can download for free at <http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp>

It's also a good idea to change your network connections so that your TCP/IP protocol is not bound to the Client for Microsoft Networks. You can learn how to do this at <http://www.grc.com>. See <http://grc.com/su-bondage.htm>. This makes it harder for people to hack in over NetBios port 139 (yet if you have a good firewall, they won't be able to in any case).

For more information on your internet connection, the winipcfg and netstat commands are useful. These can be accessed from the START/Run box or from DOS if you're on a Win 98 or older operating system.

Also, it is possible to circumvent any proxy you are FORCED to connect through (for instance maybe if you live in China or the Middle East), and it is possible to connect through two proxies, making you even more anonymous (though the real test of anonymity is whether the proxy keeps logs or not).

To circumvent a FORCED proxy, or connect through two at one time, download HTTPPort at <http://www.htthost.com/>. The program is only 760MB, small enough to email as an attachment. Details on how to use it are here: <http://mikhed.narod.ru/en/programs/httpport.htm>. Basically in the proxy server box of your browser (Internet Explorer, etc.) you point your browser to what is known as the localhost, 127.0.0.1 on port 3128, then in HTTPPort, you put the FORCED or FIRST proxy as the proxy you need to bypass, (if it's a forced proxy it will usually connect on port 80) and in the "Port Mapping" section of HTTPPort, the local port is 3128, while the subsequent remote port and remote host are your second proxy and its respective port.

So HTTPPort first goes on, circumvents, and connects you to the forced proxy which you normally would automatically connect to. Then it goes through your browser, which connects to the local host, 127.0.0.1 on port 3128, then back to HTTPPort which connects to the second proxy and its respective port, which allows you to surf freely.

The only thing is, can the forced proxy detect HTTPPort?? Because it looks to me as if HTTPPort is the PROGRAM which connects you to the forced proxy (however it would most likely be very easy to spoof HTTPPort and make it look exactly the same as Internet Explorer).

HTTPPort will make you connect through one proxy, and then make that proxy connect through a second proxy. Just as if you connected through one proxy, and then went to <http://www.anonymizer.com>. I guess that by using HTTPPort and then going to a proxy webpage you

could connect through three or more proxies. If you're FORCED to connect through a proxy, HTTPort makes your forced proxy connect to a second proxy which bypasses the censoring.

Also, remember your browser is just a software program running on your computer. Given this, it could be quite possible to manufacture another software program like HTTPort which allows you to connect through 3 or 4 or 10, or 100 or more proxies if you chose to. It could be made to work in with your browser. Though conceivably you could still be traced if all the proxies kept logs, and if you have one proxy which doesn't keep logs, you would only need that one proxy. Normally when you connect through your browser, you go through the proxy or first computer, and then your browser sends a command to connect to the website or second computer, so proxy chaining is just the same, and quite conceivable.

Also, it may be possible to turn your home computer into a proxy for other people to use, though I'm currently unsure of how to do this. It may be possible with a program called "Wingate" yet if you're not careful it may at the same time open your computer up to hackers. However I've heard that Linux users are able to proxy through each other's computers.

Also, as far as encryption goes, I was thinking about this, and I guess if you connect to an encrypted WEB site, only the website can see the information which you are sending to it. If you first connect to a non-encrypted proxy, and then to an encrypted website, your ISP could still see which site you connect to IF they packet read, because the first "GET" command would not be encrypted. But of course, your ISP wouldn't be able to see the encrypted information, (unless they have de-encryption keys) and the connection would be encrypted from the website to your own computer, even over the proxy. So the proxy doesn't really help anything. Yet if you connect to an encrypted PROXY such as <http://www.megaproxy.com>, your ISP can't see anything (except that you're connecting to megaproxy, BUT, any information sent between the proxy and another website is not encrypted. So for instance if you write a note to a message board while using megaproxy, it COULD conceivably be intercepted by anyone on any router which the packet travels over from the PROXY to the website (though not from your computer to the proxy), since you do not have a secure connection with the website and your connection is only encrypted between your computer and the proxy).

Really, who are you evading? A website, or your ISP. So encrypt to evade your ISP, and proxy to evade a website. And connecting to an encrypted website ensures your information is not intercepted by anyone on any of the routers which your information travels over to reach the other computer.