Title:
How To Make Sure That Your Pc Is Protected Against Attacks

Word Count:
524

Summary:
When you go on the internet, you have to give certain bits of information to be authenticated by the protocols that make the web work; this makes it possible to advertise who you are, where you're connecting from, and if you're not careful, a lot more. Among the information that's handed out freely is your IP (Internet Protocol) address, generally in the form of four sets of numbers separated by periods, the country your ISP is located in, often times the origination of your ...

Keywords:
Go To My PC

Article Body:
When you go on the internet, you have to give certain bits of information to be authenticated by the protocols that make the web work; this makes it possible to advertise who you are, where you're connecting from, and if you're not careful, a lot more. Among the information that's handed out freely is your IP (Internet Protocol) address, generally in the form of four sets of numbers separated by periods, the country your ISP is located in, often times the origination of your TCPIP stack, which tells someone if you're on a Mac, PC or Linux box, your browser type used, and, because of browser caching for speedy access to previously hit sites, your browser history.

If your computer doesn't have certain functions turned off, it can be even worse. For example, unblocking the port of Windows Messenger (not to be confused with MSN messenger) will get your computer spammed with a thousand little gray boxes that all need to be turned off. Some computers and their TCP/IP stacks support finger and ident, which can reveal your personal information online. Even innocuous web sites that ask you for registration information can have that information intercepted and passed around.

If you're concerned about handing out your personal information on the web, be aware that there are ways to surf the web anonymously. This cuts the trail of breadcrumbs and bits that lead potential identity thieves back to you. The first way to do this is to route through an anonymous proxy server; this replaces its

IP address for yours, making it harder to track your IP address – and with hiding your IP address, a lot of the foundation for needless information exchange gets removed.

The primary vendors in anonymous proxy servers are for-pay services; these offer a wider and mostly secure range of products. Most also have a free version for people to try the benefits out; this has a number of benefits to you – you get to see what a difference it makes – and for them, because they can tell you about the benefits you'd accrue with the paid service. The top vendors are ShadowSurf and Guardster. For both of them, you log in, and enter the URL (web address) you want to go to. Given how internet search engines are willing to sell your search data to federal agencies, and police organizations – even foreign governments – it's better to be prepared than to rely on the anonymity of the herd. In this vein there is another service called Anonymizer, which is designed specifically to help internet users bypass government mandated censorship and filtering.

An anonymous proxy server won't fully protect you against viruses and malware; it will make it harder for you to get them by browsing the web, and a lot of what they do can also be done by adjusting your router settings and the Network Abstraction Layer. If you're concerned about people knowing what you browse, though, an anonymous proxy server is a definite must. You must also make sure that the proxy server is really an anonymous proxy server. Use proxy servers from countries with high regulatory standards.