Browse the Internet Anonymously

may 30, 2012 by freecomputerzone • leave a comment

Each day we hear about another case where private information was compromised online. We've heard of thieves hacking into websites and stealing credit card numbers or people stealing personal information from bank databases in order to steal your identity. We hear of government computers committing errors and releasing private information. And now we are hearing more than ever of malware being spread via websites and email that allows hackers to compromise your computer and steal your private information and financial details. The issue of protection while browsing the internet is becoming more and more important. This article offers steps to help protect your privacy and aid you in browsing the internet anonymously. free.

Every time your computer communicates with the internet, you leave a trace of what you did and where you came from. Every time you browse the internet, send an email, transfer files, you are leaving behind electronic fingerprints that can trace your data, location, and possibly your identity. We are not here to spread paranoia or to scare you from using wireless networks or the internet. In fact, by simply understanding the limitations, risks, and how to safeguard your data, you can enjoy the internet safely and protect your identity.

When you open your internet browser (be it Internet Explorer or Mozilla Firefox or Google Chrome), you are leaving a host of details on your PC regarding what sites you visited and in some cases usernames and passwords used to log on. This can be particularly alarming if you are using common-use public computers such as those in an internet cafe, a public school, a hotel business center, or in the office where you may share computers. Get 25% off Anonymizer Universal . This coupon expires in 7 days, get it now !

What can you do about it?

If you are browsing the internet from home, protect your connection to the internet – make sure you secure your wireless network . Next, secure your browser. You can do this by tinkering around with your Internet Explorer security settings. A safer alternative to Microsoft's Internet Explorer browser is to download and install the Mozilla Firefox browser or Google Chrome browser – both are secure (and free).

There are three ways to go about protecting your privacy while online:

1. Browse normally, then, once your are finished, cleanse your computer by removing traces of where you went to include your browsing history (list of sites you visited) and cookies (fingerprints that are deposited on your computer from sites you visit). Lastly, you will have to delete your temporary internet files.
2. Or, you can browse through a specially-equipped internet browser that covers your tracks AS you browse and leaves no trace on your PC as to where you went and what you did online.
3. Either of the two above options will still reveals your IP address (numerical address that locates your internet connection) to the websites that you visit. You can mask this by utilizing an anonymous proxy service to browse the internet. You can combine this with either of the two options above to maintain the highest level of anonymity.

What is an IP Address?

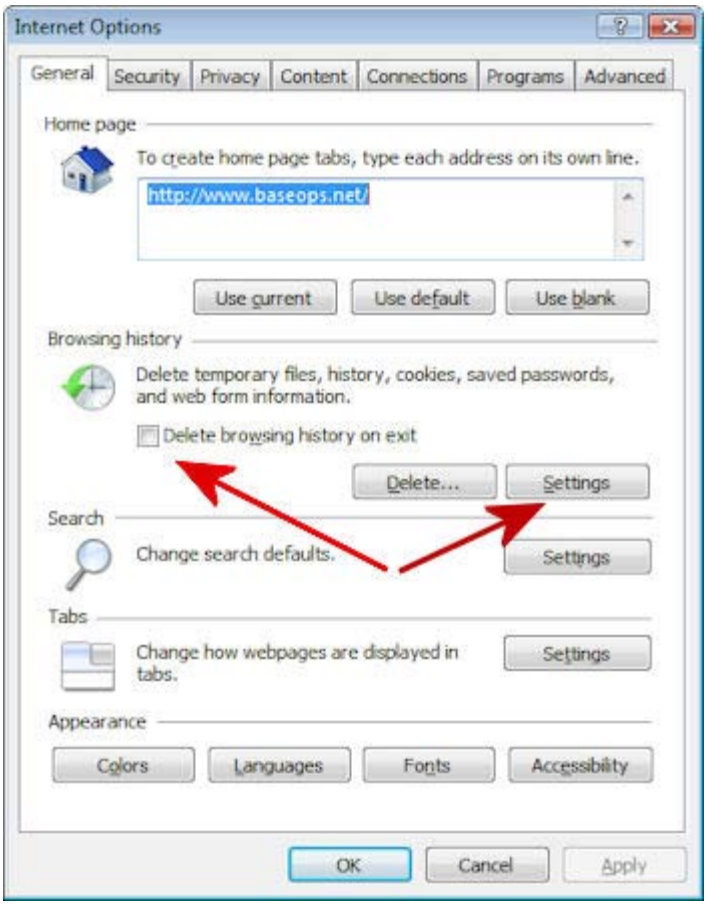
An IP address is the Internet Protocol address, a unique numeric identifier for a computer on a network. It is a way to identify your internet connection's approximate geographic location.

What is a Proxy Server?

A proxy server is a server or software that gives the appearance that a user is browsing the internet from a location other than his/her true location. A proxy server can mask your true IP address.

Configure your Internet Security Settings

Select Internet Options in your browser. In the General tab, you have the option to adjust how your Browser History is handled (see image below) – you have the option to manually delete your temporary internet files, browser history, cookies, and saved passwords (click on the Delete button); you can even have select to have these items automatically be deleted every time you shutdown your browser (select the "Delete browsing history on exit" check box). In the Security Tab, you can adjust the overall level of security of your browser as well as customize these settings. In the Privacy Tab, you can control individual



aspects of your browser as they relate to privacy.

Tell your Browser you want to Browse Anonymously

Both Internet Explorer and Google Chrome internet browsers have native built-in modes that allow you to browse anonymously. In IE it i

s called InPrivate Browsing – go to your toolbar and select the "Safety" tab, then from the drop down menu, click on "InPrivate Browsing". In Google Chrome it is called Incognito Browsing – click on the wrench symbol in the upper right, then from the drop down menu, select "New Incognito Window".

Use an Anonymous Proxy Server

You can hide your true IP Address when browsing the internet by logging on through an anonymous proxy server. A proxy is basically an intermediary website that opens a secondary window allowing you to browse to any website THROUGH their website. The benefit here is that your identity (IP Address) is masked and instead of showing your home location, your IP Address mimics the proxy's address – which can be another city or even another country. Typically, browser speed and connection bandwidth are limited when using a proxy, but your physical location is masked. Protect your identity & surf anonymously. Try Anonymizer Universal™ now!

Often we find ourselves traveling on the road. Many business travelers will bring their own laptop or netbook computers with them when they travel. However, there are still many times when a traveler needs to use a public computer such as those found in a hotel business center or internet cafe. This may be due to a lack of wireless internet connectivity in your hotel room, or the need to use the public printing services available at such locations. Additionally many business travelers and military personnel find themselves traveling overseas where their

personal laptop may not be able to connect to that country's internet, and they are forced to use a public computer to access the Internet.

Many people when placed in this situation, are often hesitant to use such public computers to access the internet, especially if personal or sensitive data such as financial records, are being transmitted (e.g. paying bills online). There are, however, ways to safeguard your privacy when using any public computer to access the Internet.

Protect your Privacy when using Public Computers

First, unless absolutely necessary, avoid entering any personal information on a public computer internet browser, to include any user names or passwords, addresses, financial information, or anything else that can distinguished you from other users using that public computer. If that is not practical, and you must enter such personal information in your course of business, or due to other needs such as the necessity of paying bills, there are still things you can do to protect yourself.

You may find yourself in a hotel room, or at an internet cafe, or a friend's house and have the need to log on to a financial website such as your online bank or other bill pay site. Fear not, there are still things you can do to protect your personal confidential information when using a public computer.

1. Open the internet browser and log on to your banking site.
2. When you are all done, make sure you log off of this website (click on the "log off" link at the top of the page). Do not simply visit another website or simply close your browser – make sure you actually log off.
3. After you have successfully logged off (and received the logged off message on your screen), click on TOOL in the upper right of your internet browser, then select INTERNET OPTIONS (on Microsoft Internet Explorer). Next, click on DELETE BROWSING HISTORY (see image above for a screen shot).
4. Next, close-out the internet browser – do not simply visit another site, but actually close your internet browser.
5. That's it! Make sure you follow all of the above steps. You still cannot be certain what software or malware has been installed on a public use computer – use your best judgment. If you are in a reputable hotel in a good neighborhood, etc., you are probably in much better shape than not. Be especially wary of using a public computer in a foreign country as most Westerners are monitored when visiting foreign countries.

The Ultimate Anonymous Browsing Solution

If you don't have one already, purchase a USB flash drive. On that USB flash drive, download and install a portable Internet browsers such as Mozilla's Portable Firefox. Portable Applications are streamlined applications that can be installed on any media including a memory card or thumb drive, and do not need to run off of the computer's hard drive. Thus, you're able to use the portable browser installed on your thumb drive to access the Internet. Any personal information you enter into the browser is contained wholly within that little browser which is on your thumb drive. No personal information or trace of where you browsed will be left on that public

computer. The minute you "eject" your USB flash drive from that public computer, all your personal information and browsing history is removed as well.

Additionally, having a means to protect your user name and passwords is also a smart way to protect yourself. Since these are public-use computers, you have no idea what type of software, good or bad, as they installed on that computer. Although not certain, it is possible that there may be software on that computer designed to steal personal information or passwords. To protect yourself, store your user names and passwords and a separate encrypted file, located on that same USB flash drive.

One piece of software we highly recommend is a freeware program called Steganos Locknote . This is nothing more than an encrypted text file that stores any text that you enter in and save. The entire file is encrypted and password protected. Other more complicated pieces of software include password managers. One such popular and free password manager is KeePass Password Safe . These programs are designed specifically to store your usernames and passwords. By using Locknote or a password manager such as KeePass, you can avoid having to manually type in each username and password as you visit sensitive sites such as a banking web sites or anything else where you have to enter your personal data. Instead of manually entering and your username and password through the keyboard, you can simply copy and paste your username and password right out of Locknote or your password manager software to connect directly to your browser and the website you're trying to visit. This is a safe way to defeat malware such as keystroke loggers that try to capture information a user types in through his keyboard.

Suggested Reading List:

1. How to Browse the Internet Safely
2. How to Protect your Privacy Online
3. Free Hard Drive Encryption
4. How to Encrypt your Wireless Network
5. Advanced PC and Home Network Security

.....

Steganos Locknote - This is an application and document in one: the mechanism to encrypt and decrypt a note is part of it. Secure, simple, independent. No installation required. It appears as a simple text file and opens to look just like a file in notepad. The only difference is that the contents are encrypted and secure. And you can have as many of these different "Locknotes" on your computer at one time. A great place to secure your username and password combinations since the file is encrypted, lightweight, and no delay in loading.

CCleaner is a very useful and user friendly software that allows for even novices to keep a healthy computer. The basic program is very small and free to download. Consider using CCleaner to maximize efficiency and

productivity with any personal or family computer. The main cleaner is able to analyze and delete superfluous information. This includes things like temporary internet files, internet histories, cookies and recently visited URLs.

The registry cleaner allows users to scan for missing file extensions for preloaded programs. This can be used to help restore issues where a person may have accidentally deleted necessary files for the computer to run. There is also a feature which displays a Startup list where users can enable or disable various programs that initially start when the computer is first turned on. Another very convenient feature is the system restore that allows for a person to reset the settings to a previous date and time if the computer becomes infected with a virus or malware.

Related Posts:

1. Protect Your Privacy on the Internet
2. Surf the Web – Anonymous Proxy Server

filed under: privacy • tagged with: anonymous internet

Speak Your Mind

Name *

Email *

Website

Post Comment

Google™ Custom Search Search

Protect Your Privacy

Fix My Computer

Fix Common Problems

Remove a Computer Virus

Increase Laptop Battery Life

Secure Your Wireless Network

Create Windows Repair Disk

Update PC Drivers

Remove Browser Hijack

Re-Install Windows OS

Buyer's Guide

Backup Hard Drive Guide

New PC Buyer's Guide

Printer Buyer's Guide

PC Discount Coupons

HP dv7t High End Laptop

iPad versus Netbook

HP dv6z Budget Notebook

Custom Order PC Online

How-To Articles

Startup Your PC in Safe Mode

Back-Up Data to the Cloud

Build Your Own Website

Upgrade Your Laptop Hard Drive

Wireless Home Network Windows7

Setup Windows7 HomeGroup

Create a Windows7 Restore Point

Customize Browser Security Settings