The Anonymity Tutorial, a revised version!

Author: Raven, founder of SWG.
URL: http://www.securitywriters.org

Note: this tutorial deals with privacy issues on the net, and how to improve your anonymity, not how one can find details about another person. This topic is discussed in the Information Gathering tutorial, which is the sequel to this tutorial. Issues such as under what conditions some of the details that can be found about you according to this tutorial can be obtained and how to conduct such privacy intrusions will be discussed in the sequel tutorial.
In the mean time, you can read a little about the dangers themselves and more about how to avoid them and improve your anonymity on the net. Happy reading!

Preface: ph33r the net

Whether you realize it or not, the Internet is not as anonymous as you might think. Here are a few examples:

1) You enter a website. Once you hit any one of the files on the webserver, the website owners can find out these pieces of information about you, and much more:

1. Your IP Address.
2. Your hostname.
3. Your continent.
4. The country you live in.
5. The city.
6. Your web browser.
7. Your Operating System.
8. Your screen resolution.
9. Your screen color depth.
10. The previous URL you've been to.
11. Your ISP.
12. Your Email address.
13. Your MAC address. (don't know what a MAC address is? Everything will be explained later)
14. What kinds of browser plug-ins you have installed.

15. Wether you have Java and Javascript support turned on or off.
16. Any information that is stored in your cookies file. (don't know what cookies are? Everything will be explained later)
17. Other private details.

And that is just the tip of the iceberg.
Can you guess who gives away all of this information? Well, I'll give you three guesses... your web browser? Yes, that's correct, your web browser gives a lot of information about you because some websites use this information to customize the page depending on your resolution, screen color depth and more, and some sites read the last URL you've been to in order to know whether you reached that page from the author's site or whether you reached that page from a different site (meaning that some other webmaster is "leeching off" their files). Other websites use this information for other purposes...

Just to show you how much information your browser gives away, let me show you how a typical MSIE HTTP request (a request from an HTTP server to download a page or a file) looks like:

```
GET /texts/internet%20security/anonymity.html HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, */*
Referer: http://www.www.securitywriters.org/networking_security.html
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
Host: 62.0.96.180:8011
Connection: Keep-Alive
```

See what I'm talking about?

Guess number two... TCP/IP itself? Yup, true, TCP/IP itself provides the website with your IP address and your MAC address (this part will be explained later on), which can then be used to find your hostname, which can be used to find your place of living or at least where your ISP is located.
Guess number three... the user itself? You guessed correctly again, my friend. Wow, you're really getting the hang of this! ;-) Anyway, the point is that lots of stupid users tend to trust every site with their private details and fill every form they see without making sure that the site has a valid privacy policy.
So what can we do about it? Well, a lot. But let's leave that to later, shall we? We will discuss anonymous surfing in the anonymous surfing chapter.

2) Another example: you're connected to an IRC network and you are chatting with your friends. Right now all a person who is connected to the same IRC network needs in order to find information about you is nothing but your nickname. He doesn't even have to know you, or be in the same channel/channels you are. Here are a few examples of what anybody can find out about you (in the most optimal conditions) by simply knowing your nickname:

1. Your real name.
2. Your Email address.
3. Your IP address.
4. Your hostname.
5. Your ISP.
6. Your continent.
7. Your country.
8. Your city.

And again, there could be more. The reasons? You name it. TCP/IP, the IRC protocol, Silly users...
There's a lot you could do in order to improve your anonimity on IRC networks, but we'll discuss this issue in it's appropriate chapter.

The same goes for online games, instant messengers, Usenet networks, Emails and everything else you do on the net. Have I convinced you yet? :-)
Some of you are anxious to continue reading and improve their anonimity. Others have been convinced that the Internet is not anonymous, but don't see why they should make any efforts to anonymize themselves - don't worry, you will be given reasons, just keep on reading. And last but not least, some of you may still be skeptical about whether doing all those things and finding all of this information just by having someone visit your web site or finding someone on ICQ really is possible - for people like you and other curious boys and girls, I have written the information gathering tutorial, which can be found at www.securitywriters.org's texts library as well. It will teach you how to do all of those things and much more!

Chapter I: testing yourself

So... how anonymous are YOU??
Yes, you, right there, on the other side of the monitor. What, you think I can't see you? This is the Internet, not Television! Yes, there's a monitor and there are pictures and sounds and issues of public interest, but it's completely different! The net controls you! The net owns you! Everything you say, everything you do, it's all recorded and stored permenantly on a hundred thousand different servers on the Internet! They control everything - your computer, your TV set, your phone, your car, your air conditioner, your nearest Supermarket's price scanner... even your underwear! They know anything and everything, they know me and you, and they

know EXACTLY what you've been hiding in your socks drawer (naughty naughty you!).
The above part was completely unnecessary. I just felt like rambling. Anyway, this chapter lets you, the reader, venture into the depths of the net (how melodramatic) and try a few simple tricks on himself. Let's begin with something easy: a web search.
Point your browser to www.WhoWhere.com. Now, see if you can find yourself, and see what kind of information you can find about yourself. Try the different searches, and click on anything you see. I managed to find my name, Email address, home address, home phone number and much more, and I suspect that some of the information was given by my ISP, and the rest was given by GeoCities.com, which I signed up for (sometime in 1996, I think) when I built my first web site.
Now let's try something else. We've already concluded that web browsers send out a lot of data about you, and that web servers can run software that logs this information and saves it for later retrieval. But even people who own small websites and don't have access to the actual server and can't install such software on it or access it's logs can still get all of this information about their visitors by subscribing to online web statistics services. One such service is SuperStats, so point your browser to http://www.superstats.com/.
At SuperStats and other such services, Webmasters can sign up, and then put a small portion of HTML code into any of their site's pages and the web stats provider will kick in and do the rest whenever someone enters that page. The process is fairly simple: the code contains an instruction to the web browser to retrieve a certain image from the webstats provider's server. When your browser retrieves that information, it leaves it's footprint in the webstats provider's server's log files (web browsers give away a lot of information, remember?) and they do the rest of the work.
Anyway, that site has a "live demo" button which can show you just what kinds of information this service (and other similar services) can capture.
I have just found a web page with a list of "environment variables checkers". These are scripts that get those variables that your browser gives away, and can show them to you. Check that page out at http://proxys4all.cgi.net/env-checkers.shtml, follow one of the links and see how this web script (and any other web site) can find those details with extreme ease.
Now let's try some Emails. Send an Email to yourself, and when you get it, access it's full headers. With MS Outlook, you can do that by right-clicking on the message in your Inbox and clicking on properties. With Netscape Communicator, this can be done by clicking view, the headers, then all. So, now you can see how Emails really look like, and guess what? They contain loads of information about you! They can tell anyone who receives or intercepts an Email from you lots of details about you, including the Email client you're using and your operating system (these details can be used to send OS-specific of mailclient-specific viruses to your mailbox, which could infect your computer), and of course many other details such as your ISP, the area of your living and more.
For further information about mail headers, please read
http://www.securitywriters.org/texts/internet%20security/tracemail.html and
http://www.securitywriters.org/texts/internet%20security/mailspam.html

See how easy it is to find information about you? And that's just the beginning.

Chapter II: the first step in anonymizing yourself - Anonymous Surfing

Why would you want to surf anonymously? Let me give you a short reminder, and explain the situation a bit further.
First of all, we concluded that TCP/IP hands in your IP address, and this address can be used to find out who your ISP is, and possibly track your geographical location (wanna know how? Then the information gathering tutorial at www.securitywriters.org is just for you!).
Now you must be asking yourself "why does TCP/IP give this information if people can use it to find all of this information about me?". Well, the answer is quite simple. TCP/IP has to put your IP address in the IP header of the packets that you send, because otherwise, how would the server that you are requesting the web page from know where to send it back? If your packets won't contain your IP address or will contain a fake address instead, you won't receive the returning packets.
However, there's a workaround for this. What if you could tell some sort of a public computer to retrieve the files for you, and then have the public computer send the files to you? That way, the IP address that will appear in the packets will be the address of the public computer, and your IP will remain anonymous, right? This is called bouncing, because you send the packet to the public computer, and then the public computer sends the packet to the web server, so your packet metaphorically "bounces" from one computer to another in order to hide your true address. I will explain how to bounce a connection to a web site in a few minutes.
The other problem with TCP/IP is that it gives away your MAC address too. Oh, wait, I haven't explained what a MAC address is!

Info Break: What is a MAC address?

A MAC (Media Access Control) address (also called an Ethernet address or an IEEE MAC address) is a 48-bit number (typically written as twelve hexadecimal digits, 0 through 9 and A through F, or as six hexadecimal numbers separated by periods or colons, i.e. 0080002012ef, 0:80:0:2:20:ef) which uniquely identifes a computer that has an Ethernet interface. Unlike the IP number, it includes no indication of where your computer is located. To learn more about MAC addresses, head to WhatIs.Com's definition of a MAC address at http://whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212506,00.html.

Now, why a dial-up Internet user would have a MAC address is really beyond the scope of this tutorial, but the point is that you have such a thing, and since it's a 48-bit number, there are billions of different combinations and your MAC address can be used to identify you (not in a very reliable way, but it has a good enough success percentage). This form of

identification can be used to track your online shopping habits, for example (it is known that some online retailers pass this kind of information from one another). So in other words, exposing your MAC address isn't too good either.

So, the second privacy risk we talked about was your browser giving all this information about your computer, right? And of course, your cookies file is being exposed to the entire world. Wait, I haven't even explained what cookies are yet!

Info Break: What are Cookies?

Webster dictionary defines a "cookie" as:
1 : a small flat or slightly raised cake
2 a : an attractive woman <a buxom French cookie who haunts the... colony's one night spot -- Newsweek> b : PERSON, GUY <a tough cookie>
3 cookie : a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a Web site server, and containing personal information (as a user identification code, customized preferences, or a record of pages visited)

Uhh... ignore the first two. So that's what a cookie is. Web sites can instruct your web browser to save information into your cookies file. Ever been to a site that has a login prompt that offers you to "remember" your password? That's how it works - your password is saved in your cookies file.
Looking for more information about cookies? Then I suggest that you follow this link:
http://whatis.techtarget.com/WhatIs_Search_Results_Exact/1,282033,,00.html?query=cookie

Now, the problem with the cookies file is that every site can read it, not just the site that stored the cookie entry in the first place. Today, most sites save passwords and other kinds of sensitive information in an encrypted form, but encryptions can be broken... so if you're entering a suspicious site, you might want to access your browser's preferences and disable cookies, so the suspicious site won't be able to read them.

Now, for the workarounds for these problems:

How to surf anonymously

There are several ways to surf anonymously. Each way has it's pros and cons (advantages and disadvantages, respectively), and blocks different kinds of information from leaking out.

The Anonymizer

This is probably the easiest way, but also the least convenient way.

What is the Anonymizer: Anonymizer.com is a service that is given to the web community for free, and can be upgraded for a certain amount of cash. Anonymizer.com is also a completely anonymous ISP (costs money. More information about this is available at their web site).
How to use: simply go to www.anonymizer.com and type in the address that wish to go to.
Pros: * blocks EVERYTHING - IP, browser information, cookies, anything.
* Easy to use.
Cons: * blocks EVERYTHING (what if you wanted to have cookies support or any of the other things that Anonymizer blocks off? Oops...)
* Annoying ads and page delays, but you can remove them by signing up to their premium service (costs money).

Anonymous Proxies

A more convenient way, but only blocks your IP and your MAC address.
What are Proxy servers: Proxy servers are bouncers that are meant for people like you and me who want to surf anonymously. They will create the connection to the web server for you, therefore eliminating all the privacy issues that derive from TCP/IP, but they won't protect your cookies file (unless you disable cookies in your browser's preferences dialog box), and they won't block off all of the information that your browser sends out.
However, Proxies have another purpose. Some ISPs have a Proxy server that caches (stores on it's hard drive) web sites. The Proxy allows the ISP's users to use it, and when someone attempts to retrieve a web page that has already been cached on the Proxy server's hard drive, he can receive the files he requested directly from the Proxy server (MUCH faster). The Proxy updates it's cache memory several times a day, to make sure that it has the most recent version of the websites it cached. Such Proxies can only be used by the users of the ISP which owns the Proxies, and they usually aren't anonymous.
How to use: first of all, you need to find a web Proxy. You can find several working ones at Cyberarmy's Proxies list (http://www.cyberarmy.com/lists/proxy/) or at Proxys4All (http://proxys4all.cgi.net/. This site also has links to some other web-based Proxies like the Anonymizer). Then, once you have a Proxy's address and the port that it uses to accept connections (usually 8080 and 1080), you need to configure your web browser to use it (just access the options/preferences page and the rest should be a piece of cake).
Note: if web pages suddenly become unavailable, it means that your Proxy server has gone down (it was shut off, moved to a different address or no longer accepts connections), and you must find another Proxy server.
Pros: * very easy to use - Once you have found a Proxy and configured your web browser to use it, you won't have to worry about it anymore.
Cons: * doesn't block the information that your web browser hands out.
* Proxies can sometimes go down or stop accepting connections from you for different reasons, and you'll be left alone in the dark (until you switch to a different Proxy or stop using Proxies at all).

* Using Proxies can sometime result in slower loading times, if the proxy server is overloaded.

Chaining Proxies

More security, but longer load times.
What is chaining Proxies: remember I explained about bouncing? So if you can bounce your connection over a Proxy server, why can't you bounce your connection over several Proxy servers? Your packets can bounce from one Proxy to another on a line. This is called chaining Proxies.
How to use: it seems that different proxies can be chained in different methods, but most Proxies can be chained by separating their addresses with -_-. E.g.:
http://proxy.spaceproxy.com/-_-
http://anon.free.anonymizer.com:80/http://www.securitywriters.org. Try it!
Don't like this method? Fine, you can also tell your browser to set up chaining for you so you won't have to type those long addresses. For more information regarding how to do that and pictures explaining exactly what to do, head over to http://articles.etecc.com/chaining.php.
You can also try using a program called Webonycer. I uploaded it to securitywriters.org, and you can download it from http://www.securitywriters.org/webonycer.zip. This program can make some peoples' lives a lot easier.
Pros: * Better security. If someone would really want to trace you, he will have to go through a lot more effort to track you down.
Cons: * Makes pages load much slower (your packets go through a longer route with each Proxy in the chain).
* You become dependant on more Proxies, so if one of the Proxies in the chain goes down, then not only that you will need to find another Proxy, you will also face a new problem - you won't have a way to tell which Proxy went down (unless you test each Proxy manually).

Surfing from a Shell Account

Slower, does not allow graphics but hides EVERYTHING.
What is surfing from a shell account: you can connect to a free shell account provider and use Lynx, a text-based web browser to surf the net. This is another form of bouncing, because again, you request another host on the Internet to retrieve the website for you, and it sends it back.
How to use: the easiest way is to connect to a telnet server such as the one at the University of Kansas. Click here (telnet://ukanaix.cc.ukans.edu) to telnet in, and then log in as www or lynx and you'll be able to use Lynx to browse.
Pros: * Hides EVERYTHING.
Cons: * Hides EVERYTHING (in case you didn't want to hide some of the details or use your cookies).
* Slower than direct surfing (like every kind of bouncing).

* No graphics support (this is Lynx, after all. It does not support graphics, and neither does it support Java, Flash and other things that require a graphical display).

Those are some of the things you can do in order to surf anonymously. Of course, there are other methods - there always are. I tried to give you a general taste of the mostly-used methods. If you wish to learn more about this topic, the web is wide-open, and web searches (especially at google.com, which is by the way my favorite search engine) could find you everything. And of course, there's always SWG's web forum (http://www.securitywriters.org/forums.html), with the quickest responses in the world (questions are usually answered in an hour or less). If you ever face a question which you cannot solve by a thorough web search, come over to the Q&A forum and me and the rest of the Q&A staff will happily help you out.

P.S. don't forget the third reason for privacy intrusions: stupid users! Make sure that a site has a privacy policy before you enter any private details into a form!

Chapter III: Internet Relay Chat - can it be anonymous?

IRC, Internet Relay Chat, is a great way to expose yourself to the world. Really, IRC and privacy don't go well together. However, online privacy on IRC has been steadily improving.

The Risks of IRC

Any common IRC'er can easily fetch several details about you. First of all, there's your IP address. Anyone could type /whois your-nick and see your IP address. Furthermore, that person can also initiate a DCC (Direct Client Connection) connection with you for a file transfer or for a DCC chat session and obtain your IP by using a program that comes with every Internet-enabled Unix/Linux/Windows installation - netstat. Netstat allows you to view every connection made by or with your system over the Internet, and its status. Once you accept a DCC request from an attacker, he can find your IP because there is a direct connection between you and him, so netstat would show your IP.

But the fun doesn't stop there. There's also a big deal with the details you provide the IRC server with, such as your Email address and your real name, if you have entered those details. There's also the risk of compromising your passwords: several IRC services, such as chanserv and nickserv (don't know what these are? Read SWG's IRC guide. You can find it at SWG's Texts Library), require you to enter a password which you can choose by yourself. When choosing your password, *DO NOT*, I repeat *DO NOT* choose the same password that you used for something else. In fact, it is advised not to use any password twice anytime, anywhere, but IRC is one of the worst places to use a password twice.

If someone manages to get your password by either breaking into the IRC server or by

pretending he's an IRCop and asking for your password, he could use this password to gain access to anywhere else you may have used this password (other services, your Email account, your web site, your shell account etc'). Also, it's quite easy to turn in your password by mistake. Many times I have seen people typing in their passwords into a channel instead of into a message window, thus revealing their passwords to practically the entire world!

Anonymizing yourself on IRC

There are several steps you can take in order to assure your online anonymity on IRC:

1. Don't type in your real name and your real Email address when your IRC client asks you to, unless you want them revealed.
2. Don't use any passwords you use on IRC for anything else.
3. Choose IRC networks that hide your IP address! Also, when connecting to a new network, read the motd (Message Of The Day) by typing /motd and see if there's anything about hiding your IP address. IRC servers that claim to hide your address usually spoof the last part of your address (the last 8-bit digit), like that - 62.0.75.spoofed, which is enough in most cases.
4. Do not accept DCC requests from people you don't know. Even if the IRC server hides your IP, it will be revealed through a DCC connection since DCC is direct, and does not go through the IRC server (that's why it is called Direct Client Connection).
5. Many servers hide your real IP address, but some require you to tell them to do so. In order to do that, you must type either /mode your-nick +x (replace your-nick with your nickname) or /mode your-nick +z , depending on the server.

If you want further anonymity, you may also want to use suid.net, the world's only (as far as I know) encrypted IRC network. It is also considered secure because of the considerably low number of netsplits, but that's beyond the scope of this tutorial.

Chapter IV: ICQ - the worst thing that ever happened to privacy

ICQ is considered by most to be a security threat to its users. During the course of its evolution, it has suffered from many serious bugs and vulnerabilities, such as vulnerabilities that allowed malicious users to probe another user for a lot of information, or to launch attacks with serious effects, ranging from flooding the user's ICQ client with messages, causing it to crash, stealing his password or even breaking into his computer.

Vulnerabilities have come and gone, but many have stayed. During this tutorial, we will focus on the simple vulnerability, which is caused by the way that ICQ works, and therefore hasn't been patched. It's the vulnerability that allows anyone to view your IP address, and it exists because ICQ is a client-to-client program.

Even if you tell ICQ not to reveal your IP in the preferences dialog box, under privacy, there are other ways a malicious user might try to find it other than looking at your info and expecting to find it there. Since ICQ is a client-to-client program, messages and other ICQ events are transferred directly from one host to another, without the interference of a server, meaning that if you send someone a message or someone sends you a message, a socket is created between your computer and the other person's computer. What does this mean? This means that anyone who sends or receives an ICQ event from you can use programs such as netstat to view all existing connections, spot the one that belongs to you and get your IP address!

Go ahead, try it. Press start, run, and then type command. A DOS window will appear. Type netstat -A and you will receive a list of existing connections, their status and other basic information about them, as well as the IP of the other host which is connected to you through that socket (unless this is a listening socket, which is waiting for a host to connect to it. A listening socket will not give you a "Foreign Address".

So why doesn't Mirabilis change that? Why doesn't it change ICQ so all events are transferred through the server, so attackers will send and receive events to and from the server and thus will be unable to find other people's IPs? Simple. Because what kind of a mad man would want all those millions of ICQ users moving their traffic through his server? And though AOL (the current owners of Mirabilis) has a lot of money and can probably pay for all this bandwidth, why would they do that? They don't care about your security, and they won't spend an extra cent to improve it. As a result to that, new versions of the ICQ client are released without being properly tested, and new holes are being frequently discovered.

Of course, the fault is not Mirabilis's alonel. There are also several user-inherent problems, caused by users that reveal private information by writing it into their user account info. Everyone can view your info, so don't reveal anything that you wouldn't like to when you fill out the form in the ICQ account preferences dialog box.

Chapter V: Electronic Mail - encryption and headers

Email, too, is not as innocent as it may seem. In order to teach you why, and how to make your Emails a bit more anonymous, you should learn about Email headers.

E-mail headers appear at the top of every Email message that you receive, although you may not see them unless you tell your Email client to show them (Outlook users: right-click on the message in the inbox window and choose properties, then details. Netscape Messenger users: press view, then headers, then all). Email headers contain all sorts of details, some of which are collected by the SMTP server which the sender used to send his Email, some have to do with the process of the delivery of the message and some are other details, like the MID (Message ID). Let's take a typical header for example:

```
Envelope-to: raven@mail.box.sk
Received: from [194.90.1.9] (helo=mailgw2.netvision.net.il)
by dwarf.box.sk with esmtp (Exim 3.20 #1 (Debian))
id 155wUP-00015d-00
for <raven@mail.box.sk>; Fri, 01 Jun 2001 23:29:50 +0200
Received: from ***sender's name removed*** (ras1-p88.hfa.netvision.net.il
[62.0.96.88])
by mailgw2.netvision.net.il (8.9.3/8.9.3) with SMTP id AAA14549
for <raven@mail.box.sk>; Sat, 2 Jun 2001 00:32:06 +0300 (IDT)
From: "***sender's name removed***" <***sender's address removed***>
To: "Raven" <raven@mail.box.sk>
Subject: securitywriters.org
Date: Sat, 2 Jun 2001 00:24:30 +0200
Message-ID: <MABBIBPFAKENJLPBHEDLAEAHCAAA.***sender's address removed***>
MIME-Version: 1.0
Content-Type: text/plain;
charset="windows-1255"
Content-Transfer-Encoding: 7bit
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200
Status:
```

Well, that's nice. Look at all this information which is hidden in every Email message you send! Everyone with a bit of knowledge about Email headers can find out lots of details about you. Of course, I had to remove the sender's name and Email address in order to preserve his privacy, but I left the rest of the details untouched.

So, what do we have here? Except for the regular details (sender's Email address and his name, which he defined for his Email client when he first configured it), we also have the sender's IP address (or the IP address he had while he sent the mail, in case he has a dynamic IP address).

Another thing you should do if you wish to achieve maximum privacy is to encrypt your Emails. That way, you can assure that noone who intercepts your message in one way or another, or breaks into the recipient's Email account will be able to read it. PGP is the most common mean of encrypting Email. Get it from PGP International.

Info Break: What is a dynamic IP address

Dynamic IP addresses, as opposed to static IP addresses, change every time you go online. While users with a permanent connection have a static IP which does not change, dial-up users and other kinds of users which don't have a permanent connection receive a different IP address each time they go online.

But that's not all. In addition to the sender's IP address, we can also tell what Email client software he used (unless he forged these details, but that's beyond the scope of this tutorial. If you wish to learn how to do that, consult Raven's Introduction to Complete Newbies and Hacker Wannabes, Episode I). There are several steps you can take in order to hide those and other details about yourself.

1. Use an Email client that doesn't identify itself (there are several ones on the net. Do a web search), or send Emails by connecting to an SMTP server with Telnet and sending the Emails manually. If you wish to learn how to do that, consult the Hack FAQ.
2. Use anonymous remailers.
3. Use any other method of bouncing your connection, such as bouncing it over a shell account or a Wingate computer or any other kind of proxy that will allow you to bounce a connection to port 25 (that's the port which SMTP servers listen to, and that's the port an Email client connects to when sending Emails).

Chapter VI: Usenet - not just news anymore

Once a huge Internet community, Usenet is now known by a very small percentage of the users in the world. Usenet is like a BBS, which is a Bulletin Board System. Basically it's very much alike today's forums, which every self-respecting site or portal now has. Messages, also known as articles or posts are stored in a central database where users can browse through the articles to find the piece they want. Indexing and cross-referencing options are also available. This is very helpful because it is easy to find the information you need, and it's much more convenient to have a central server than having all of this content stored on your computer.

By posting to Usenet, you reveal your Email address. This means two things:

1. You cannot post anonymously.
2. You are very likely to receive junk mail.

How do we get rid of that problem and post to Usenet while keeping our Email addresses private, then? Well, there are several methods.

1. Use a commercial service for posting messages anonymously. Some are free, some cost money, but anyway, it's worth it. I recommend trying services such as www.nymserver.com, www.mailanon.com (has a 7 day trial period) and www.deja.com.
2. Don't post with your real Email address. Instead, open up another address for posting on Usenet at Hotmail, for example.
3. Use a mail-to-news gateway service to post. Such services allow you to post to Usenet by Email. But instead of sending your Emailed posts from your real address, send it from a fake address or using an anonymous remailer.
4. Last but not least, some of the services listed above will still reveal your IP address. In order not to reveal it, use a proxy server to bounce your connection over it, so only the proxy's IP address will be revealed.

Chapter VII: Spyware

Since the collapse of the NASDAQ, software companies have been trying to find new ways to make money. They realized that shareware doesn't work - most people prefer not to buy the full program or download a crack for the program and get all of its features rather than to pay for it, and only a few people actually buy software. Several solutions were invented. One of those is Adware.

Adware is software that contains advertisements, which earn revenue for the software company that distributed the program. However, the Internet advertising business is sinking, and advertisers pay less for advertisement space on the Internet. This is why Spyware was invented.

Spyware is a program that literally spies on its user. There are different kinds of Spyware programs, which differ from one another by the kind of information they collect. Some collect information about what kinds of programs are installed on your computer, others collect information about your surfing habits and others may get your Email address and the addresses of all those in your address book and sell them to spammers for tons of cash (as far as I know, the standard fee for a thousand valid Email addresses is approximately 100$). As far as I know, some may go as far as recording conversations you have over the Internet.

This information is later sold for a lot of money to different companies that may be interested in this kind of information (trust me, there are a lot). This is bad because:
1. This hurts your privacy.
2. Transmitting the data which the program collected wastes your bandwidth.

To fight Spyware, you can use programs that detect and remove Spyware from your computer, such as OptOut and Ad Aware. You can find these programs at every self-respecting download site.

Here's how to remove Spyware:

There are many online forums, chatrooms and websites that deal with Spyware. Google.com, the best search engine in the world (in my opinion) lists over 32,000 different webpages that mention the word Spyware at the moment, and that's a lot, considering the fact that this is a relatively new topic.

Many sites offer lists of Spyware programs and information about them (including information on which files to remove in order to disable the program's spying abilities). Do a web search, you'll find plenty.

Chapter VIII: Browser History, Cache, Cookies and Autocomplete

Your own Internet browser can turn you in! Imagine what would happen if your girlfriend would find out about all those sex sites you surf to, or if your boss would find out where you've been surfing while you were supposed to do some work, or some idiot posting some embarrassing items out of your browser's history. Unless you know how to properly clean your browser's history, you'd never know when you'd get caught with your pants down (literally).

Your browser's cache database is also a problem. But first of all, we have to understand what cache means.

Info Break: What is cache?

Cache is defined as a storage area that contains data that your computer will need to use in a short time. There are different hardware and software that use cache. For example, every modern CPU (Central Processing Unit) has a cache memory chip installed next to it, which stores data that the CPU will need shortly. Accessing the cache is much faster than accessing any other kind of storage device, and takes a lot of load off your RAM.

Internet browsers also use a certain form of cache memory. They save web pages, including pictures, on your hard drive. Then, the next time you access those sites, your computer will access the site from the local cache instead of from the Internet. In order to assure that the version of the site which is stored on your local cache on your hard drive is up to date, your browser compares the size of the files in your cache to the size of the files on the web server and download whatever has been changed. If you wish to download a site from the Internet completely and overlook the local cache, you can either set your browser's preferences to do so or press Refresh (IE) or Reload (Netscape).

The size of your browser's cache can be limited to a certain amount, if you wish to save disk space, but know this about any kind of cache space - the bigger, the better.

Now that you know what your browser's cache is used for, you have probably realized that cache is a privacy risk. People can search your cache memory to find out which sites are cached, therefore learn where you've been surfing recently. However, unlike clearing your browser's history, clearing your cache has a drawback to it - you'll have to download the pages that were deleted from your cache again the next time you go there instead of being able to load them from your cache.

Another risk is cookies. We've already established what these are in the first chapter, so let's suppose that you know what they're for. So obviously, if you have a cookie that, say, saves your username and password for some sex site so you won't have to type them in every time you enter the site, won't anyone who is able to lay hands on your cookies file know that you've been there? Unfortunately, clearing your cookies has its drawback as well - you'll have to delete all those stored preferences and passwords, so do this only if you wish to obtain maximum privacy at this high cost.

And finally, there's another risk that only exists for IE users. This is called Autocomplete. Autocomplete is a new IE feature that allows IE to remember what you typed into web forms and allow you to enter the same data into them the next time you visit that site in a mouseclick. I'm sure you can already imagine what huge privacy risks this involves...

I will explain how to clear your browser's history, your cache and your cookies to IE and Netscape users, and how to turn off Autocomplete to IE users, since these are the most common Internet browsers. Those using other browsers will have to look up information on their own.

How to clear your browser's history:

There are several ways to do this. First of all, you can do this manually. Instead of explaining here, I've decided to refer you to this site, because it has images along with the explanations of how to clear your history. Make sure that the cleanup removed the records of the sites you've been to both from your history page and the address pulldown box, which also shows the last places you've been to.

If you'd rather automate the process, you can use a number of very useful tools, such as Evidence Eliminator (a very famous program. It also cleans up other kinds of evidence that don't have anything to do with Internet surfing), Cover Your Tracks, Don't Panic, Siege Washer, Webwasher (a personal favorite) and ComClear (for those who use Netscape under Linux and other Unix variants. Has both a graphical, GTK+-based interface and a textual interface). Many of the programs listed above can also delete your cookies and clear your

cache.

How to clear your browser's cookies:

Cookies are very easy to get rid of. The safest way to get rid of your cookies is to delete the cookies file, a plain text file often found somewhere under the directory where your browser has been installed. If you wish, you can also use programs such as Deleting Cookies, which does the job.

How to clear your browser's cache:

To delete your cache, just do as follows:

Internet Explorer users, go to the Control Panel, then choose Internet Options and choose to delete your temporary Internet files (that's how IE calls your cache).
Netscape users, go to the preferences dialog box, then open the advanced category, click on cache and choose to clear both the disk cache and the memory cache.

How to turn off Autocomplete:

Open up Control Panel, click on Internet Options, then go to the advanced tab and remove the tick mark from Autocomplete (turned off by default).

A Final Word

The object of this tutorial was to teach you how unsafe the Internet is and how many privacy risks there are on the net, in hope to educate the average net user to become more aware of risks and take steps to improve his privacy.

I believe that online privacy is very important, because if your computer is exposed, everyone in the world can peek in. Just like you won't give away your house key to strangers, you should preserve your anonymity and privacy on the net. After all, it's your right.