Mr Anonymous

Leaving footprints on the sands of time may all be very well, but not if it happens to be quicksand you are treading on…

Photograph: IRA AWASTHI
Digital Imaging:

Reality is getting overcrowded. The shopping mall, the library, the cinema, the nearest picnic spot, the telephone booth... there is no place where you can relax and do your own thing at your own pace.

Except perhaps the Internet. Log on, and—yippeee!—You are in your own private world.

Or are you?

If you are one of those who regularly use e-mail for correspondence, meet friends in chat rooms, participate in serious Usenet discussion forums, trade online stock exchange or surf porn sites on the sly, chances are that you have already left enough information about yourself on the Net for Andrew Morton to write a two-volume biography.

And if that still does not worry you, this will:

ιA company in the US claims to provide a kit that teaches you how to get information about your employees, neighbours, friends, enemies and others. This kit, which sells for about $18 (less than Rs 800), also shows you how to access unlisted phone numbers, locate social security, birth, adoption and death records.

The threat is not from the teenage hacker, but somebody closer home.

ιIn 1995, Russian crackers hacked into a Citibank server and credited $10 million to their account.

ιA hacker named Carlos Felipe Salgado confessed to stealing 100,000 credit card numbers from the Net.

ιPixar, the company that made the movie *Toy Story*, was mail-bombed by a person who claimed to be Steve Jobs. The e-mail contained payroll details of the employees working for this organisation.

ιPharmaceutical companies in the US are trying to create a databank of medical history of every living person on this planet. Your next employer may check up your biography on the Net before hiring.

The threat is not from the teenage hacker, but somebody closer home. It could be your ISP provider, the new rival across the street, a disgruntled employee or even free software.

Beware of freebies

Any 'service' that is free—e-mail accounts, Usenet newsgroups, access to special information, and downloads—is always welcome. But accept such offers with care. Apart from your name and e-mail address, some service providers would want you to send personal information like residential address, phone number, social status (whether student or employee), hobbies and other details. And this is where the trouble begins. Most first-time surfers volunteer real information. Getting this information is child's play for data thieves like spammers and crackers.

These virtual criminals run certain software that can collect details about you from newsgroups, e-mail service providers, FTP sites and other services. Once they have the information about you, you could be conned into responding to junk e-mail that says you can avoid further mail by replying to the sender with the word 'remove' (or something similar) in the subject line or text of your mail. If you take the bait, you unwittingly end up confirming that your e-mail is genuine.

That's not all. Sites such as DejaNews archive all postings from Usenet. By simply entering your e-mail address, anyone can obtain a list of all newsgroups that you are a part of. And thus, they can obtain your profile and interests. Services such as PointCast track the links you click on, and highlight your interests in order to deliver customised advertising. All this information is stored and retrieved by advertisers who can then clog your mailbox with offers and discounts that you would perhaps never be interested in.

Also, in certain cases, your browser may automatically leave your e-mail address behind when you download software from an FTP site.

Unlawful entry

The other, more common way is to break into your PC. There are many ways to hack an individual machine or a network. For one, the browser you use may have a security hole. This allows a remote site to access the contents of your PC through the use of ActiveX, Java or JavaScript programs.

These crackers are interested in getting hold of the information the Web browser stores on your hard drive—this need not be limited to the history of sites you have visited. They also track the pages and the pictures that you view. Enabling cache options stores entire files downloaded from Web sites. Cookies—programs that track all the sites you visit—maintain details of newsgroup activities, including the number of messages you read (sometimes the messages themselves) and the newsgroups you visit.

If you think the future of the Internet is brighter and safer, think again. With the advent of high-speed broadband technologies such as cable modems, the relative security offered by dial-up modems seems to be fading. The modem is replaced by an Ethernet card. Ethernet cards are primarily used in LAN networks that are not usually wired to the outside world. Hence the IEEE 802.3 and derivative protocols that accompany an Ethernet card work on the premise that all connections are 'trusted'. But when used with cable modems, it makes your PC accessible to anyone using the same services. By simply knowing the name of the machine as presented to the Ethernet, (the default name for all computers is 'My Computer') a stranger can access or change any or all of the files on the victim's computer.

Look before you log on

Since you cannot avoid being online, it would help to exercise some caution to ensure that information about you is not easily accessible to people.

Encryption: When you frequently need to send important documents via e-mail or messages on chat, use encryption software. Many of these are available as freeware. Use a corporate digital signature on your e-mail for authentication. You can also use folder- and file-encryption tools. These will ensure that even if a hacker swipes a file from your hard drive, it will not be useful to him. (*For more about data encryption, see 'In a Jumble' CHIP June*)

Encrypt voice communication: Using programs like SpeakFreely (freeware) you can encrypt voice communication by using algorithms that require two groups to set a secret key before they start talking. The program is extremely compact (less than 300K) and allows the users to select any compression protocol provided; some of which are compatible with those widely used in other Internet telephony programs.

Firewalls: For corporate organisations and institutions, the only security against Trojan sites is a Firewall. This will ensure that while you surf the Net, the Web sites you visit will deal with the proxy server or the firewall server and not with your PC, so the data on your hard drive remains safe.

Spam busters: Never open an e-mail message that has the word 'Free!' in its subject line. Not even if it offers a free PC! Spam mail slows down your mail server or boots you out of your e-mail account. Though some e-mail accounts have in-built filtering facilities, a reliable anti-spam software will do the job better.

Surf smart: Create different e-mail accounts for different purposes. Use Web-based e-mail for personal use. POP mail provides better security and management features. In case you want to subscribe to an unknown or free service, create another e-mail account where you don't reveal your identity.

Use different passwords: Assign separate passwords for multiple e-mail accounts or Net services, and remember to note them down. Do not use names or birth dates for passwords or use password-generating software. Most sites have the password reminder feature, which allows you to type a question that leads you to your password. Here, do not use commonly - known personal information in reminder question.

Play hide and seek: There is more than one way to surf the Net incognito. For example, you could use a commercial service for posting messages. It costs money, but it is convenient and easy to use. (Try www.nymserver.com and www.mailanon.com. The latter offers a free 7-day trial period).

You can also disable your browser's cookie function (if you don't mind losing some functionality) to avoid personal information being stamped at every site you visit.

Set up a dummy e-mail account for Usenet discussions. This effectively prevents people from guessing who you are, but if you want to conceal your location as well, you should use a proxy server when posting the message–or your IP address will show up in the Usenet message header and give you away.

While transacting business on the Net, use a separate credit card, preferably one with a credit-locking facility.

Use Re-mailers: A re-mailer is a company, organisation or private party that has configured their computer to receive e-mail message from you, then re-address it and send it to the person you want to send it to. In the process, they remove any headers that might point back to you. There are many re-mailers on the Net, some of them let you put a fake return address, but most of them directly state that the message was sent from an anonymous source.

You might have been using the Internet taking little or no precaution to protect your privacy, but it is never too late to learn. Start by taking a back up, and format your hard disk. Open new e-mail accounts. Install encryption software. Empty your cache everyday. Work smart and incognito and enjoy safe surfing. Remember, better safe than sorry!

P RAGHUNATH