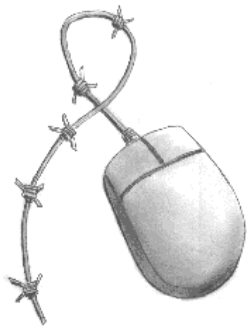
Participating With Safety Briefing no. 6

Using the Internet Securely



Written by Paul Mobbs for the
Association for Progressive Communications, March 2002.

This briefing is one of a series on Information Security. It looks at:

- How the Internet can be used to monitor your online activity.
- Minimising the risks to your online activity being monitored.
- Minimising the risks to your system
- Privacy and system maintenance
- Common ways we expose our identity on the Internet.
- Managing disclosure: Alternate personas

The Internet is an open network; any point on the network can be accessed from any other. This is what makes the Internet a publicly accessible mass medium. It also makes using the Internet a security risk - through the information you give out, and through the opportunities it gives other people to impact upon your work.

The Internet presents three main risks, in decreasing order of significance:

- ***Exposure of Private Information -***
  When you send email and browse the web, you are not anonymous. You leave logs of what you have done on many servers. People can also put 'taps' on your email connection and record all your incoming and outgoing email and web traffic.
- ***Damage to your computer -***
  When you are online or use internet services, you expose your computer to computer viruses and hackers.
- ***Unwanted public profile -***
  It is becoming easier to rapidly compile profiles about people and their online behaviour from bringing together information they disclose about themselves as they use the internet.

Organising your information and your computer system well and having a good back-up system are the best ways to protect your system (see especially briefings no.2 on *Backing-up Information* and no.5 on *Computer Viruses*). But learning how to work online in a way that protects your information, your identity, and if possible your privacy, is an important part of working securely on the Internet.

How the Internet can be used to monitor your online activity

Connecting a computer to the outside world, through a local network or the Internet, turns it into a potential tool of surveillance.

Sending and receiving private information on the internet is challenging. The process of sending an email is

similar to the process of sending a real (physical) letter. Imagine you are sending a real secret letter. If you leave an early draft of the letter at your house, someone might find it. If the postman cares, he might notice who you are sending it to, and how heavy the envelope is. If the postman cares a lot, he might open the letter and read it. The postman will then deliver the letter to the local post office. Again, the post office might record who sent what letter to whom and on which date, and they might even open the letter. You local post office will send the letter to the post-office nearest to the recipient, and finally on to the recipient himself. If the recipient leaves a copy of the letter lying around, it is possible the letter may be discovered.

The risks for email are greater than the risks for real mail. In the above metaphor, your postman is your connection to your Internet Service Provider (ISP). Your post office is where you have your email account, and how you send outgoing mail. The recipient's post office is the recipient's email provider, and the recipient's postman is the recipient's ISP. But it gets worse! In the internet, email providers always, automatically log who sends email to whom. And, by default, our emails are like a postcard - the message itself is easily visible to the postmen and post offices.

Everything you do on the internet goes through your ISP. The default for most internet services is to send everything in 'cleartext'. This means that, for example, the entire contents of your email is visible to anyone with access to your local network or the connection to your ISP. It is also possible for you to protect certain services by setting up automatic encryption of the service. For web-browsing, you can use the secure 'https' protocol instead of the 'http' protocol. 'https' is the standard for all online banking websites and most 'log-in' pages. There are webmail systems that use https as well. If your email service provider has SSL capability, you can 'tunnel' securely past your ISP to receive and send email. This is called POP/SSL and SMTP/SSL. Of course, you still need to trust your email provider to a certain extent.

Briefing 4 in this series explains encryption. It is possible to send emails encrypted with an encryption programme such as PGP. However, this only encrypts the body of the message. The headers, such as 'From', 'To', and 'Subject' and all still visible to your ISP. These headers can be used to monitor the activities of groups or individuals; it enables a watcher to generate a profile of what an individual or group of individuals have been doing together online, what other systems or email addresses they have contacted or have been contacted by, and the times, dates and even locations of when the members of a 'network' communicate.

Here is an example of an encrypted message. You can see that the 'header' information is not encrypted. The Header is in bold. You can see that a lot of information about the message is not encrypted.

```
Delivered-To: an-email-list@seven.gn.apc.org
Received: from nfs1.gn.apc.org (nfs1.gn.apc.org [194.202.158.5])
  by seven.gn.apc.org (Postfix) with ESMTP id 3BBC23957
  for <an-email-list@seven.gn.apc.org>; Mon, 7 Jan 2002 09:58:52 +0000 (GMT)
Received: from KBLAP.gn.apc.org ([194.202.158.101])
  by nfs1.gn.apc.org (8.9.3/8.8.8) with ESMTP id KAA17178
  for <an-email-list@gn.apc.org>; Mon, 7 Jan 2002 10:02:03 GMT
Message-Id: <4.3.2.7.2.20020107095742.028fc888@pop.gn.apc.org>
X-Sender: person@pop.gn.apc.org
X-Mailer: QUALCOMM Windows Eudora Version 4.3.2
To: an-email-list@gn.apc.org
From: a.person <person@gn.apc.org>
Subject: Re: [an-email-list] new member
Content-Type: text/plain; charset="us-ascii"; format=flowed
Sender: an-email-list-admin@gn.apc.org
Errors-To: an-email-list-admin@gn.apc.org
X-BeenThere: an-email-list@gn.apc.org
X-Mailman-Version: 2.0.6
Reply-To: an-email-list@gn.apc.org
List-Help: <mailto:an-email-list-request@gn.apc.org?subject=help>
List-Post: <mailto:an-email-list@gn.apc.org>
List-Subscribe: <http://mailman.greennet.org.uk/mailman/listinfo/an-email-list>,
```

```
  <mailto:an-email-list-request@gn.apc.org?subject=subscribe>
List-Id: <an-email-list.gn.apc.org>
List-Unsubscribe: <http://mailman.greennet.org.uk/mailman/listinfo/an-email-list>,
  <mailto:an-email-list-request@gn.apc.org?subject=unsubscribe>
List-Archive: <http://mailman.greennet.org.uk/mailman/private/an-email-list/>
Date: Mon, 07 Jan 2002 09:59:37 +0000
X-UIDL: 6cc!!S;n"!LjD"!~L-!!

-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 7.0.3 for non-commercial use <http://www.pgp.com>

buqZ7/TNFRl5HU+Nenl+dOchFoAzh4rQTea/AFUlhdy3XLXTORAxb8vme9NM8YIP
sM4RE73ByoS/ll/lLrb3GG4QsX51GIiVwO6J0HzXGEbsQqcmQDdVLe2P7FDokI4r
UvhO+Q2oHn9oiE/JRxz5OHprwl2ThvXsxRhKvIXiszzkzxSoEG1D9gLci44iy47P
crzGA1pfOZIAgifhHeQtk4mseUO4BSlbRk1/K1HAbeJ9lSc+mVEL3V2tLxT3Eq6x
ggNnhiyqYcnAkTw2FKvaYsHmrOH0cnxfypFjBvNiQEk0qq5rr4lJQ8ItIlr2lzSE
0XRXT+2GkIELlpuuY2U2BpYs7wAHPO8hp+nQTQQscSttE2utleC4n958DUE5w3zU
Zd+S0Rqy7M6J6CJcAc4AVPK4X5A2abrsttVxEdeNXDvDIdAbfFHpm0qHqoB2iUKl
MbL+y9k+mPXVe6eRzb6j47/by/PuYLlE8i1cVVvYACMbjfIJAtukFMRFqsDp7EWu
pz9NPB4wCEL4qXQpMUHbM9FlVkmNJ3Y5UINsIxsWlU241AZi+vPk1x/saLclN5Kd
JgoGkQaHLVvhKvAACdISgojemFfaCDe+buZ+qimBfhLj6GnadTMk84oIlX9j6evm
f4zHj354IjQ2aGOrqdCoO6sn7LVR2VaXP0U2/O5Vy/zPn1dPy4kY2JsqeN/30nX8
WN8CAce0l2WWvJE=
=LZSS
-----END PGP MESSAGE-----
_____________________________________________
an-email-list mailing list
an-email-list@gn.apc.org
http://mailman.greennet.org.uk/mailman/listinfo/an-email-list
```

Minimising the risks to your online activity being monitored

There are a lot of online services and software that you can use to improve your privacy.
The next page has a matrix of common tools. This is followed by advice on when to use these tools.

Secure Email

If you are sending and receiving email by your ISP, they can potentially read all your email. This may or may not be acceptable. If security is a concern, there are several options you can consider.

Examples of free, somewhat private web-based email are:

S-Mail Setup an web-email address with http://www.s-mail.com. This system lets you check your email on the web using the fairly-secure https protocol. If you send email with s-mail, your ISP will not be able to see what you have sent. However, if the recipient of the email is being monitored, your email may not be secure. If you correspond with people regularly about sensitive issues, you may ask them to get an account on the same system you are using.

Lokmail As an alternative, if you are emailing someone who uses PGP, you might be interested in http://www.lokmail.com/. Lokmail is similar to s-mail.com, and lets you access it via https. But it also lets you encrypt your messages to people using PGP. It has a server-side PGP system (that is, Lokmail encrypt your mail as opposed to you doing so with your mail programme). But, this is not as provably secure as using PGP on your local computer.

Common Anonymity, Encryption and Information Management Tools

Name	Location	Cost	Type	Remarks	Good for / recommended use	Bad for / drawbacks
Encryption						
Hushmail	http://www.hushmail.com	Free	Web based email with encryption	Java-based	On the road: Email encryption Emergencies recommendation: Have an account there	Only encrypts to other hushmail users Slow on dialup
s-mail	http://www.s-mail.com	Free	Web based email with encryption	Java-based like Hushmail, but faster, no expira-tion time and less trustable	On the road: email encryption Emergencies recommendation: Have an account there	Only encrypts to other s-mail users Slow on dialup
Cotse	http://webmail.cotse.com/helpdesk/support/smtppop.html	$5.95/ mth	Mail and other privacy tools			
Zixmail	http://www.zixit.com	US$ 24/ year	Encrypted email		Can send private email to users of standard email	
LokMail	http://www.lokmail.net	Free	Web based email with standard PGP encryption	Does not use Java Can send encrypted mail to any PGP user		
PGP	http://www.pgpi.com	Free for non-commerc ial use	General encryption (email, files)		Everyday encryption needs Recommended for Windows OS	License required for non-personal use Moving to a closed product
GnuPG	http://www.gnupg.org	Free	General encryption (email, files)	Does not use patented algorithms	Everyday encryption needs Recommended for non Windows OS	Windows OS support is basic

Name	Location	Cost	Type	Remarks	Good for / recommended use	Bad for / drawbacks
Anonymity						
Anonymizer.com	http://www.anonymizer.com	Tunnel-ing: US$30 /3 mon-ths	Secure tunneling anonymiser	SSH based solution, so encryption is included	Anonymize all kinds of communication (smtp, pop, http, etc)	Anonymous publication
nethush	http://nethush.com	Free (basic) 15 US$/ month (gold)	Web anonymiser	Web browsing only.	Anonymous web browsing with url encryption The free version is better than safeproxy.org for web	
Safeproxy.org	http://www.safeproxy.org	Free (basic) 5 US$/ month (gold)	Web and (web-based) email anonymizer			
TriangleBoy	http://fugu.safeweb.com/sjws/solutions/triange_boy.html	Free	network against blocking (censorship)	Peer to peer technology	Accessing sites that have been blocked by your ISP	
Anonymous remailers	Changing often. See: http://www.sendfakemail.com/~raph/remailer-list.html	Free	Email anonymizer	Completely email based	Offline anonymous email sending	
Tools						
Cyber Scrub	http://cyberscrub.com	US$ 40 - 60	File wiper and trace remover		Better evidence deleting than PGP	Only for Windows
APC Rapid Response Network	http://www.apc.org/english/rights/alerts/index.shtml	Free	Mirroring network for threatened content		Sites susceptible to censorship	
The Freenet Project	http://freenet.sourceforge.net	Free	Network for publishing content freely / anonymously	Requires propietary client for publication/ browsing		Requires propietary client for publication and browing
Various remote file storage tools	www.globedesk.com www.freedrive.com groups.yahoo.com www.streamload.com	Various	Remote file storage	Yahoo groups offers 20 Mb for free	Off-site backups	
Spam Mimic	http://www.spammimic.com	Free	Message hiding (stegano-graphy)	Hides short messages on spam-like messages	Hiding the existence of a message	Does not really encrypt the message

S-mail and Lokmail are free, easy to use, and fairly secure. However, they are not as provably private as PGP or Hushmail (which is described in the next section). The reason we recommend s-mail instead of Hushmail is that Hushmail terminates free user accounts if they are not used for 3 weeks, and Hushmail takes longer to start than s-mail. If you have very strong security needs, or do not trust s-mail or Lokmail, you should consider using Hushmail's paid service or using the 'Paid, more private' option below.

If you only need to send secure emails every once in a while, but you need very strong encryption, Hushmail is a good option. Hushmail uses very strong encryption, and is easy to set-up and use. But you must pay for the Hushmail service if you require regular, reliable use.

If both you and the person you are communicating with use Hushmail, no one can monitor what you say. However, Hushmail can be slow to use over a dial-up phone line.

Hushmail terminates free accounts if they are not used every 3 weeks. If you want other people to be able to contact you securely, you could subscribe to the paid Hushmail service and advertise your Hushmail email address. You can set your Hushmail account to alert your normal address that you have a new message waiting in your secure Hushmail account.

Another option is paid, private email using clients like Microsoft Outlook, Eudora, or other email programs that can work alongside PGP. PGP is 'the standard' in secure email. PGP uses very strong encryption (see Briefing 4), and your ISP will not be able to unscramble the contents of your messages.

However there are obstacles to using it effectively:

- It can be hard at first to understand about how PGP's system of public and private keys work.
- It is sometimes difficult for your communication partners to use PGP.
- Even if you both use PGP, your 'traffic data' of From/To/Subject is still visible to anyone watching your internet traffic, as is the fact you are using PGP. By looking at this traffic data, anyone watching will be able to see who you are emailing, what the subject is, and that you are using PGP. Who you are emailing is often important information for those monitoring your activities

To avoid the last problem, you need to use POP/SSL and SMTP/SSL to email providers that you trust not to divulge your traffic data. There are many web-hosting and email providers who offer POP/SSL and SMTP/SSL as part of a web-hosting package. If your email providers accept SSL connections, it is quite simple to set your email client options to use this functionality.

The final option is anonymous, private email. Sometimes people need to send an email message and make sure no one can tell who sent it. This is not easy to do.

To get around the problem of traceable email 'anonymous remailers' have been developed. These receive email with forwarding addresses included and forward the email on to the recipient. It then appears as if the email originated by the remailer, rather than the person sending it. Some systems also allocate random addresses that allow a reply to be sent back. But, in the last few years, many of these remailers have closed, sometimes because of pressure from the law enforcement and security services, but mainly because of legal threats from those who have been attacked or libelled by anonymous email.

Different remailers operate different policies. Some are truly anonymous, and will not log any data that identifies users. Others require you to open an account. Some are free, some charge for the service. Providing a reliable list of anonymous remailers is difficult because their policies may change regularly, and new ones may open as others close. You should search the Internet to find a current list of remailers. You can do this by using a search engine such as *Google* (http://www.google.com) using the keywords 'anonymous remailers'.

Many remailing/mail forwarding systems now archive the traffic which passes through them in order that messages can be traced back to the point of origin if there are complaints from the authorities. The level of privacy given to logged information will primarily be dictated by the laws on privacy and data protection in the country in which the remailer is located.

Anyone who needs to send email that is totally anonymous needs to become, or seek assistance from, a technical expert. It is easy to make a mistake and expose your identity in 'anonymous' emails. The URL listed in the matrix is a good place to start looking. *http://www.sendfakemail.com/~raph/remailer-list.html*

Anonymous web servers

Generally, whenever you use the web, two organisations know what sites you visit:

- the sites that you visit record that you visited them
- your ISP can also record what URLs you go to

You can use the web anonymously through anonymous web servers or 'proxy servers'. These stand between you and the server that you are retrieving information from:

- You request a web page from the anonymous server.
- It retrieves the page and so any information logged will be that of the anonymous server, not your own Internet service provider.
- The server will then modify any links in the page before sending it back to you. This means that if you click on any of the links in the page they too will be requested anonymously via the anonymous server, rather than direct to the server you are requesting the page from. Anonymous web servers will also log data in one way or another.

You should carefully check the credentials of the server's operator before using it!

Anonymous server relay

You should also be aware that even though you can put an anonymising server between you and a point on the Internet, the link between you and the server relay can still be tapped by your ISP.

To avoid being monitored by your ISP, you have to 'tunnel' your link to a secure server. Currently, this is only available via a paid service at http://www.anonymizer.com. There used to be another tunnelling service called the Freedom Network developed by Zero Knowledge, but it closed it's service in late 2001.

Minimising the risks to your system

Connecting to the Internet, or to a local network, can pose a threat to your system. Your system can run programs without your knowledge; unbeknown to you, they may damage your system or export information to other computers. Managing risks to your system therefore involves using programs that monitor the activity of network connections, and the activity of files or programs that access the Internet. There are two important types of program your should install - a *firewall* and a *virus scanner*.

Firewalls

An Internet connection is a two-way channel. Depending upon how your system is configured, your system may receive and process requests for other services via a 'socket' (a socket is the name for an established Internet or network connection). To limit the potential for abuse of the socket you should configure a firewall.

Internet firewalls police what programs are allowed to connect to a network socket. The network could be the Internet, or any local network that you might be connected to.

You personally have to authorise each program to connect to the socket before it is allowed to do so. Therefore any programs that are quietly trying to connect to the Internet in the background, without your intervention, will be blocked, and you will receive a warning message.

The firewall also prevents other computers on the network accessing services on your computer via the socket unless they are authorised to do so. In this way, by controlling what can flow through the socket, you control what data is allowed to flow in and out of your computer.

Firewalls can also protect privacy. As noted above, some programs try to connect to the Internet to transact information, even when you are not using the program. Programs do this by running a small program when the computer starts up. When the program detects that an Internet connection has been made it wakes up the main program to go online. Unless you have given the program permission to use the network or Internet, its attempt to access the socket will trigger a warning from the firewall. You can then deny or allow the program to access the network or Internet. This means that any rogue software, such as a virus, which has installed itself on your system, will not be able to export data from your system without you knowing about it. It also stops the 'spyware' that is increasingly built into proprietary programs in an effort to control the unlicensed use of software.

There are a number of firewalls that are available for Windows machines. Microsoft XP comes with a firewall built-in, but this only works on the incoming stream of data. Therefore programs on your computer can access the 'Net without triggering an alert. This represents a significant security flaw in the system. Most other firewall systems do monitor the outgoing data stream.

There are many free and commercial firewall programs. You can search for 'personal firewall' in a search engine, or go to www.firewallguide.com/ to see some popular ones.

On Linux systems you have many options for configuring a firewall, and most newer Linux distributions do this for you when you set up the computer.

Virus scanners

Viruses are a particular problem on Microsoft systems, where they exploit the flaws in Microsoft's programs to infect a computer and spread the infection to other computers inside files or emails. Virus scanners are a means of preventing this by warning you of potential threats to your system.

Virus scanners work by looking for the signature of a virus in a file or email attachment. More advanced systems also check your system, looking for security holes, and attempt to patch the flaws in the system.

If the scanner detects the signature of a virus it quarantines the file or email to prevent it being opened, and provides a warning to the user.

> *As new security flaws are discovered, and new viruses written, older scanners do not recognise the new viruses. Therefore it is important to regularly update your virus scanning software.*

The most important way to prevent virus problems is not to use programs that are susceptible to viruses. That means avoiding the Microsoft Outlook email program, and restricting the use of scripting languages such as Visual Basic and Java on your system.

> *Every time Microsoft introduces a new operating system it is necessary to be more vigilant whilst the flaws in the system are discovered and exploited by virus writers.*

A simpler alternative is to use a non-Microsoft operating system, such as Apple Macintosh or Linux, which because of their design are far less susceptible to attack by viruses.

Briefing no.5 on *Computer Viruses* contains detailed information on computer viruses, and how to avoid them.

Privacy and system maintenance

As noted in Briefing no.1 on *Information Security* (see the *Persistence* section) it is easy to accumulate data on a system, but sometimes quite hard to remove it.

If you use the Internet your computer will accumulate data about dates, sites and contacts that could be very sensitive.

Managing the information generated as part of your use of the Internet is therefore an important part of privacy online. The greatest threat is that your computer will be accessed, stolen or confiscated, and that the information on it will then be used against you or others. This risk cannot be removed, but it can be reduced by careful management of the system.

Email

Most email programs store data on disk. The exception is web mail, where data is stored on someone else's server (unless you save a copy to your own hard disk). Many email programs also store data separately, mainly in the files attached to an email. Often the directories associated with an email program will become clogged, mainly with useless information, unless you take care to clean them regularly. The emails themselves can also mount up, so take care to regularly tidy the 'in' box and folders of the email system.

Encryption

If you have an encryption program installed, emails that have been encrypted are automatically decrypted and displayed when you open the email.

> *Beware - file attachments are not automatically encrypted along with an email message. Attached files must be encrypted and decrypted separately, using programs such as PGP Tools (see Briefing no.4 on Using Encryption). If you have sensitive email that has not been encrypted, you might consider saving these emails as text files, and then encrypting the files using your own key, to prevent others having easy access to them.*

Web caches

Web servers, to speed up access time, store the files downloaded from web sites in a 'cache'. This cache

varies in size depending upon the configuration of your system. But unless you clean the cache regularly, particularly after doing some particularly sensitive work on the Internet, the cache will provide a detailed record of the information that you have been viewing over the past few days or weeks. It is also possible for web pages to contain information hidden in images or files that are downloaded, but not displayed. These will also be stored in your cache.

> *Cleaning the cache is therefore a simple way of clearing any data covertly hidden in web pages from your system.*

Web history files

The other significant file kept by the web browser is the 'history list'. This is a list of all the pages that have been visited recently.

You may have noticed that on some pages the links you have previously visited are a different colour from the links you have not. This is controlled by the history list. The period after which they expire is set in the configuration of the web browser. If it is set to thirty days, ever page visited over the past thirty days will be listed in the history list. If set to 'never expire', every page that the browser has viewed since it was first used will be available.

> *You have the option of clearing the history list. You should do this on a regular basis. The browser also keeps a 'bookmarks' file of links. This should be regularly edited, partly to remove any junk. When you no longer need them, remove any reference to sensitive links.*

Wiping and deleting files

As noted in Briefing no.1, when you delete files on your system it is really only the reference in an index file that is actually deleted.

> *Managing your emails and attachments, clearing your browsers cache, or editing the history or bookmarks files is not likely to actually remove these files from the system - it just removes the index entry from the file system.*

So, after doing any tidying up of files on your system, you should also *clear the free disk space* on the system. This can be done simply using utilities such as *Scandisk* and *Defrag* on Windows. But to be absolutely sure you need to *overwrite the free disk space* with new data. There are various programs available to do this, but the most effective are those that come with encryption systems. These overwrite the free space with random information to mask any data that may have been stored on the disk previously and then deleted. For further information see the *PGP* appendix to Briefing no.4, *Using Encryption and Digital Signatures.*

> *Note: To securely delete a file in Windows NT, Windows 2000, or Windows XP, you need to both securely erase the file and also wipe the free space. These operating systems use NTFS, which keeps alternate data streams of deleted files.*

Unwanted public profile

You online public identity is comprised of a number of factors:

- You may have an email address. This identifies you as a unique user of a particular computer

network; it will identify the particular network that provides your email services, and can act as a pointer as to where further information about you can be obtained.

- You may have a web site. The domain name of the web site, depending upon who registered it, will give away some information about who runs the site. By looking up the numeric address people can also find out who provides your web services, and where they are located.
- You may be a member of email list, or use Usenet newsgroups. Many of these postings may be archived, long after they were made, and may be accessible through search engines. This makes information about your interest in certain issues, as well as associations with others working on similar issues, openly available.
- As you browse the Internet you will deposit information on computers that uniquely identifies the computer you use. On the web this is managed by small files that are attached to your browser called 'cookies'. These hold small amounts of information about your use of the system, and perhaps also your personal preferences. On other systems you may have to enter your email address, which will then be used as a key to a database to track your use of the system.
- You will probably give information online about yourself in order to have access to services. Much of this information is sold to marketing companies, and is available to those who have the finances to purchase it. Although the rarest of commodities because of the costs involved, it is possible to obtain a profile of your online activities by purchasing data from the companies who harvest information from the Internet.

The greatest risk to your security is when all of the information about you is assembled to produce a profile. Hackers or surveillance operatives can gather enough information about you to make the planning of surveillance far easier. Using this information they can map your network of co-workers, identify information about you, your home, and your working habits. By researching the information that you post to the Internet, it may also be possible to gather information about your access to resources, your technical competency, and perhaps identify those who may have an interest in disclosing damaging information about you.

Managing disclosure: Alternate personas

Your identity online can be a liability. You must have an identity in order to access services that require you to register with them before giving you information. As noted above, there is the potential for this information to be used against you, stolen or abused. To solve this problem you should consider creating one or more 'alternate personas' for using the Internet.
Alternate personas are often used by people in web chat rooms. If you keep notes on the information that makes up your alternate persona, it has other uses too. To make an alternate persona you will need to set up:

- A name - this can be an alias, or just an obviously manufactured name;
- A user account - to be sure that your browser/email program gives out the correct information as part of its transactions with other server you should set up a user account under the new name (but beware, the information embedded in files may still give your main name away).
- An address - this can be difficult to make, as it should not refer to the number or name of a real location, but so long as the address has a valid street name and post code, most systems that validate addresses against postal codes will pass it.
- A new email address - this can be an additional address to your existing account, but you should make sure that your service provider does not provide information that openly associates you with this new address;
- Passwords - you will need to keep passwords that are used by your alternate persona noted down so they don't get confused with others;

- A story or 'legend' - you will need to keep a record of anything personal information you create for this persona, such as age, sex, interests, etc., so that you can supply them if required (some services validate access by you being able to enter certain personal attributes).

These details are most easily kept as a file, be it a database or word processor file, that you keep on your computer and can access when required.

> *The purpose of an alternate persona is not to provide anonymity. It is to provide a means to mask your true identity when using services online that may disclosure your personal information to others. This prevents others accessing data that could be used for something like direct marketing, but also for accessing data that could be used to organise surveillance of you.*

People pretending to be you via email

The major issue related to the protection of your identity is the securing of your *email address*. Many people also use *web mail* - email managed through a web server. Web mail produces a slightly different set of problems, but the principles are much the same.

There are three ways your Internet identity can be 'stolen':

- Information can be posted in your name, supposedly from you, but actually sent from a different address. Many people do not always read the header information that comes with a message, and may believe that the information is from you. One of the easiest ways this can be done is to concoct a message and send it as a forwarded message - so stripping it of the header information that identifies it as unique.
- Email addresses can be forged or 'spoofed'. Email servers do not always have security for outgoing emails (i.e. checking the name of the sender to make sure it is a valid account on their system). This means that the email address can be altered by changing the settings of the outgoing email address. Many email lists only discriminate by email address, and therefore if the name in the email appears to come from you the message will be forwarded to the list. Another problem is that while people will see your email address, they will not always bother to check the header information to make sure the message originated at your email server. Spoofing is a problem because in many countries it is not illegal, as long as the intention in sending the spoofed email was not to defraud the recipient of goods or money.
- Your email account can be taken over. This is far harder to do, because someone must obtain the passwords for your account. But if you do not secure your computer (especially if it is a laptop), it is possible. It may also be done by tricking your service provider into giving your details out over the phone, perhaps using information about you obtained by researching your background, guided by information obtained online. Service providers can be tricked fairly easily; they often do not know their clients personally, only by the information contained on their databases. It is also possible, but far harder, to crack your email server. Either way, these options are illegal in many countries because they constitute unauthorised access to a computer system.

> *All of these threats, with the exception of poor security on your computer, can easily be dealt with by signing your email with a cryptographic signature (for details, see the briefing no.4 on Using Encryption and Digital Signatures).*

Embedded identificationn

Computers can embed personal information in the files they use. For example, Microsoft Word keeps track of who has written and modified files.

Embedded information was originally used as a means of protecting the copyright of programs. Information that has commercial value can also contain *embedded information*, or *digital watermarks* that enable its producers to identify who used or produced the data, and therefore whether their intellectual property rights have been abused. Embedded information also provides a means of identifying individuals, storing information about their preferences, or monitoring their use of a service.

Digital watermarks and *embedded information* are an important issue within the general subject of *freedom of conscience and expression*. They may threaten our human rights to anonymously engage in dialogue, or to report facts or information anonymously. As computers and software become more complex, and with the increasing commercialisation of the Internet, anonymity is being eroded.

A further refinement of embedded information is the *online registration of software*, where the registration process is controlled by programs created by the software developer. These programs may pass on information about your computer, and the data on it.

For example, the *online registration* of the Windows 95 operating system resulted in information about the users' computer being transferred to Microsoft's systems. Microsoft's latest operating system, Windows XP, takes this process one step further. It requires that you register online, and that you divulge information about your system, in order to obtain a code that activates your computer. If you make any significant changes to your system following this, your computer will fail to operate. You must then register again, sending a new digest of information about your system to Microsoft. Because it assigns every computer a unique identity, Windows XP can also create a digital fingerprint that could be embedded into files to prove the location of the computer they were created on.

Registered or not, programs may also try to *access* their developer's computer system when you make an Internet connection. Some programs do this as a means of *checking for updates* or new offers for that program. But it also means that the program could pass on other information about your use of the computer and the program.

Causing a computer to operate processes without the authority of the user is a crime in many countries. But because for most programs you must click to accept a license agreement, you give assent to these programs commandeering your Internet connection to send data back to their home base.

The main risk from embedded identification is that a report or document you produce, and within which you have deliberately not included any identification, can identify you as its author from the information embedded within the file. Many word processors insert information on the date and time the document was produced, and allows the user to set the name of the author. But even if you clear this information, it is possible that the registration details of the program, including the name, will be encoded within the file.

> *The simplest way to avoid any risk of embedded information in a file is to use a text file. But if you require some sort of formatting you should use older file formats that carry less information, such as Word 6, or use RTF (rich text format).*

Free Documentation License:

For more information about the Participating With Safety project, or if you have questions about the briefings, contact secdocs@apc.org