ED 425 754 IR 057 254

AUTHOR	Hogle, Jan G.
TITLE	Personal Security on the Internet.
PUB DATE	1996-12-00
NOTE	19p.
AVAILABLE FROM	Web site: www.geocities.com/SiliconValley/Pines/3940/; also available as a pdf file (persec.pdf) through Website: ftp://twinpinefarm.com/pub/pdf/
PUB TYPE	Reports - Descriptive (141)
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	*Computer Mediated Communication; *Computer Security; Discussion Groups; Electronic Mail; *Internet; Listservs; Problems; *Safety
IDENTIFIERS	Computer Use; Computer Users

ABSTRACT

This document is a printed copy of the Web site written to educate Internet users about potential risks associated with communication over the Internet, and to suggest precautions to reduce those risks. An Introduction highlights why users should care about privacy on the Internet, activities that can reveal personal information to others, and types of people who might be interested in obtaining personal information. The next section lists personal information that can be revealed through the following activities: sending e-mail, posting to newsgroups and mail lists, participating in chat rooms and online surveys, purchasing products online, Web surfing, and putting up a personal Web page. For each activity, tables indicating what to do for various warning signs of problems are provided. The next two sections outline basic precautions and steps to take for extra security, and what to do should problems occur. The final section is a glossary of security and privacy terms. Contains 13 references. (AEF)

Personal Security on the Internet

This is the PDF version of the web site at:
www.geocities.com/SiliconValley/Pines/3940/

© copyright 1996, Jan G. Hogle
tabcat@geocities.com

- Purpose of this site
- Browse the Index
- Download a PDF version

Purpose of this site

This Web site was written to educate Internet users about potential risks associated with comunication over the Internet, and to suggest precautions to reduce those risks.

About this project

- Background
- References

Glossary of Security and Privacy Terms

- Intro and links to general internet glossaries
- Privacy glossary

Introduction

- Why should you care about your privacy on the Net?
- Activities that can reveal information about you to others
- Folks who might be interested in knowing your personal info

Links: Privacy Groups, Tools, and Other Information

- Books and archives
- Email and anonymous remailers
- Encryption tools
- Georgia's "Net police" law
- Organizations
- Online purchasing info

- Privacy tools and links
- Posting to Usenet
- Web browsing tools and cookie info
- WWW security links

Risks: What people on the Internet can find out about you

- Sending email
- Posting to newsgroups and mail lists
- Chat rooms
- Online surveys
- Purchasing products online
- Web surfing
- Putting up your own Web page

Remedies: What to do if you have problems

- Gather your evidence
- Assess the damage
- Contact the user
- Contact online resources
- Contact offline resources

You can print this web site or read it offline:

- Download a PDF version of this site to print out, or to read on your computer screen offline.

Note:
Adobe Acrobat Reader must be installed on your computer to open a PDF file. Adobe Acrobat Reader is a free utility for use on most computer platforms. Adobe Acrobat Reader and instructions on its use are available from the Adobe web site. <http://www.adobe.com/prodindex/acrobat/readstep.html>

Introduction

The purpose of this document is to educate Internet users about potential risks associated with comunication over the Internet, and to suggest precautions to reduce those risks.

The Internet offers a lot of information to just about anyone who has the time to look for it.

The Net is a great place to share information with people from all over the world. Unfortunately, this global information access also makes it easy to unwittingly share personal information that many people would think twice about if they really thought about it at all.

This document will help you to understand what kinds of information you make available to people when you use various communication methods on the Internet, why you should be careful with that information, and what steps to take to safeguard it.

No information is really private on the Internet.

There are many methods of gathering information about people who use the Internet, and many reasons for wanting that information. Some of these reasons are legitimate and acceptable. Others are annoying invasions of privacy, and in a few cases can even be dangerous.

Any of these activities can reveal information about you to others:

- Sending email
- posting to newsgroups and mailing lists
- participating in online surveys
- purchasing from online merchants
- logging in to a password-protected account
- surfing between Web sites

Some of the folks who might be interested in knowing your personal info:

- People trying to sell a legitimate product or service
- People who gather demographic info for marketing
- People looking for old friends, or arranging class reunions
- People researching genealogy
- People looking for an easy target to rob
- Scam artists trying to sell a product or service
- Scam artists looking for credit or account info (credit cards, passwords, phone numbers, birth dates)
- Hackers testing their skills and crackers showing off
- Stalkers looking for victims

Due to the number of people on the Net, it is unlikely that your account will be singled out.

Not all of the people who gather details about you are a threat, and you might even welcome some inquiries. It can be a lot of fun to share family history with someone researching their genealogy, or who is looking for a friend from many years ago.

However, this does not mean that you should ignore reasonable precautions, any more than you would knowingly leave your home or possessions vulnerable to burglars. There are people out there who should not have access to your personal information. Some of those people are trying to profit from scams, and some of them are dangerous.

There are simple precautions you can take, and if you inform yourself about what risks are out there, you can reduce your chance of encountering problems to a minimum.

What people on the Internet can find out about you

Common uses of the Internet and what these activities may reveal about you:

- Sending email

- Posting to newsgroups and mail lists
- Chat rooms
- Online surveys
- Purchasing products online
- Web surfing
- Putting up your own Web page

Sending email

Email can reveal a lot about you. Usually an email message includes information about:

- Your real name
- Your login ID (the first half of your email address)
- The computer where your account resides (the second part of your email address)
- The computer(s) you were connected to when you sent the email message

Depending on how you sign your email and what you include in your message, it may also reveal:

- Your address
- Phone number
- Other personal info

This is usually fine if the only person who reads your email message is the person you meant to send it to. However, email is not a sealed message like a US Postal Service letter. Many opportunities exist for unintended recipients to read your messages.

You may have heard that you should never put anything in an email message that you wouldn't put on a postcard, and you may wonder why. After all, email seems secure. You are sending a message directly to someone's password-protected account, and no one else should be able to see it without permission from the recipient, right? Wrong.

Even from a password-protected account, email is not a secure means of sending messages:

1. Email is sometimes addressed incorrectly and may reach one or more people who were never intended to receive it.
2. Email may be sent to or from a computer that more than one person has access to. Some people leave their email programs connected all day at work, and when they are not at their computers, anyone can come along and read their incoming or outgoing mail.
3. Email messages sent from your workplace can be intercepted and read by one's employer or a coworker. This is also true on the receiving end. Not everyone agrees that this practice is ethical, but it happens.
4. Email messages from work or home can be intercepted off a network during transmission using software known as "packet sniffers."
5. Email can be intercepted from a telephone transmission if your computer is connected to the network through a modem. Admittedly, this is rare, but it is a surprisingly easy procedure for a stalker to perform.
6. Email can be forged, or "spoofed," by another user who pretends to be someone they are not. Although forged mail is usually sent as a joke, it can be destructive.
7. Email can be forged by hostile Java Applets, which are also capable of obtaining your username and password.

Warning signs of problems:	What to do:
Email which never arrives, or is very slow in arriving at destinations.	Inform your network administrator, or your Internet provider.
Frequent interference with your Internet or telephone connection.	Inform your network administrator, your Internet provider, and possibly your telephone company.
Unusual or unauthorized use of your Internet account (especially noticeable with accounts that are charged by the hour/minute).	Inform your network administrator or Internet provider as soon as you suspect problems.
Email with your account name as the sender, which you didn't send.	Inform your network administrator or Internet provider as soon as you suspect problems. If the messages are harmful, report it to the police as well.
Tampering with telephone connection box (rare, but it happens).	Report the problem to your local police and telephone company as soon as you suspect problems.

Precautions to take:

Anonymous email names
Anonymous remailers
Encryption software

More Information:

email and remailers
E-Mail Privacy FAQ
encryption software
Hostile Applets
Java FAQ
privacy tools and links
phoney-mail.txt
Sniffer FAQ

- top of page -

Newsgroup and mailing list postings

Posting to newsgroups and mail lists can seem a lot like using email, and you may even use the same program to send email and postings. However, posting to a list or newsgroup is very public. Messages may be intercepted just as with email, but it isn't really necessary because in most cases your posts are being published for the whole world to see anyway.

If you would like to see just how easy it is to look at postings on newsgroups, check out the DejaNews profiles

Warning signs of problems:	What to do:
Unusual or unauthorized use of your Internet account (especially noticeable with accounts that are charged by the hour/minute).	Inform your network administrator or Internet provider as soon as you suspect problems.
Posts with your account name as the sender, which you didn't send.	Inform your network administrator or Internet provider. If the posts are to a list, report it to the listowner.
Nasty responses to your postings	Try to ignore it. If that doesn't work, contact your network administrator, or the postmaster at the offending party's email address. If you feel threatened, contact the police as well.
Responses that indicate too much knowledge about you.	It could be innocent, but if the person makes advances that are unwanted, make sure he or she knows it. Report it to the police if it gets strange.
You've posted a message to a newsgroup and now you wish you hadn't!	You can cancel your posts. Read the Cancel FAQ on how to do it.
You posted a message to a newsgroup and it never showed up, or it was there and disappeared.	If it never showed up, it may have been lost in Cyberspace or it may have been canceled by someone else. Read the Cancel FAQ for more info.

Precautions to take:

common sense posting
anonymous email names
anonymous remailers

More Information:
Cancel FAQ
email and remailers
E-Mail Privacy FAQ
privacy tools and links
phoney-mail.txt

- top of page -

Chat rooms

Chat areas can be very similar to newsgroups and listservs because they are often public forums. Chat is a little safer than newsgroups or lists in the sense that chat activity is not archived or available for later review. On the other hand, chat is less safe from the standpoint of being a "live conversation" with people who you can't see and who you know nothing about.

It is usually easy to hide your identity in chat areas. Most chat rooms encourage you to use an alias, or screen name. Since you are typing to the screen and not your email program, you don't have to worry about an email header revealing your name and email address.

Chat areas are more likely than other online communications to bring you into contact with people who are not what they appear to be. People often assume an "online personality" which can be very different from their real life persona. Remember to think carefully about what you are telling people online, and be cautious about agreeing to meet your online friends in person.

Chat encounters to be wary of:	What to do:
Requests for money	Don't send money to a stranger. Asking for money after pretending a friendship is a common scam on the Net.
Too much knowledge about you	It could be innocent, but if the person makes advances that are unwanted, make sure he or she knows it. Report it to the police if it gets strange.
Very personal or inappropriate questions	Don't answer questions that make you uncomfortable. If the person makes advances that are unwanted, make sure he or she knows it. Complain to the person's postmaster if necessary.
Request to meet in person	Try to verify who the person is, and get to know each other on the phone before deciding to meet. If you decide to meet in person, do so in a neutral public place. Don't reveal where you live, do try to bring a friend, and make sure others know about your meeting.
Unrealistic proposals, like marriage!	If you only know each other from the Net, be realistic. You need to seriously consider learning more about each other offline.

Precautions to take:

Common sense posting
Anonymous email names

More Information:
Usenet Personals FAQs
IRC Undernet FAQs
IRC FAQs

- top of page -

Online surveys

Surveys may be available on Web pages, or distributed in newsgroups and mail lists. Some folks like to answer surveys, perhaps because they like to believe someone cares about what they think. Others may participate because something is offered for free in exchange for filling out the form. Keep in mind that surveys are often used for marketing purposes, to compile lists for junk mail and advertisements, or even for scams.

Even if you don't mind sending your personal data to a marketing firm, remember that survey info can be intercepted or sniffed off the network. Try to send only basic information, like work address and phone rather than personal details. Never give out your social security number or birth date. Try to send data using encryption such as PGP or SSL where you can.

Obviously, the info you reveal in a survey can be very personal, depending on the topic. If you don't have a clear understanding of the purpose and sponsor of a survey, don't answer it.

Warning signs of problems:	What to do:
Personal or inappropriate questions.	Don't answer it.
Lack of info about the purpose & confidentiality of the survey responses, the sponsor, etc.	

Precautions to take:

- Common sense posting
- Common sense browsing
- Web security

- top of page -

Purchasing products online

When you make purchases online from a Web site, you have to consider how you will pay for the product or service. Most sellers on the Internet are honest, but some are con artists trying to illicitly obtain cash or credit card information. Sending cash to the perpetrator of a scam is bad enough, but revealing your credit card account is far worse.

Most buying and selling on the Internet is through newsgroups, and is like buying and selling through a classified ad. Methods of payment are usually checks or money orders. For larger purchases, COD is often used. You might want to read the The Usenet Marketplace FAQ for advice.

Methods are now being offered to make credit card purchases from a Web site with some security. Most involve using encryption such as Netscape 3.0 with SSL. Others, such as First Virtual offer a means to make the transaction over the telephone instead of online.

Warning signs of problems:	What to do:
Requests for detailed personal info, such as social security number, mother's maiden name, or birth date	Don't give out this info, and don't do business with folks who ask for it.
Unusual or unauthorized charges on your credit card	Follow your bank's procedure for reporting credit fraud.
A business with no physical address other than a PO Box	Verify the company's existence (physical address and phone number) before making any transaction. Check with their local Better Business Bureau and Chamber of Commerce if necessary. If in doubt, do business with someone else.
A business that asks for large payments in advance	

Precautions to take:

- Common sense browsing
- Web security

Web security

- top of page -

Web surfing and Internet connections

Even if you never participate in email, newsgroups, chat areas, or online purchases, you can still reveal information about yourself just by being connected to the net.

Finger is an Internet software program used to locate people and gather information from other Internet sites. Although many Internet service providers are now limiting incoming Finger requests to protect their account holders, it is still a common method of finding out:

- if you are currently logged on
- when you were last logged on
- when you last read your mail
- your real name
- other details, such as address or phone number (not commonly available, however)

Web surfing also reveals information about you, even if all you do is connect to a Web site and leave. You may have heard about MagicCookie and history files, which are created if you browse the Net using Netscape or Internet Explorer. Cookie and history files log information in files on your computer about:

- specific sites you have visited
- when you have visited specific sites
- how often you have visited specific sites
- the site you just came from
- the type of computer you are using
- who you are
- where you are connecting from
- email addresses you correspond with

To see for yourself what other computers can find out about you through an Internet connection, check out the Center for Democracy and Technology's Privacy Demonstration Page.

You should also be aware of hostile Java Applets. As noted in the section on email, Java Applets can forge email, steal your username and password, and all you need to do to activate the applet is to log on to a Web site. You may not even be aware that the applet is running.

Warning signs of problems:	**What to do:**
While visiting a Web site, a window pops up and asks you for your network login and password.	Some sites require a password, but don't confuse that with your network info. Don't type your network login info at a web site prompt. This may be a hostile Java applet. If in doubt, make sure you are logged off your network, then log in again.
While visiting a Web site, a window pops up and asks about sending or writing a cookie.	Cancel it, shut off the warning in your browser options, or say yes. You can delete your cookie file regularly, or get a program that will do it for you. [more]

Precautions to take:

Common sense posting
Common sense browsing

More Information:
Web browsing tools and info
Web security links and info

- top of page -

Putting up your own Web page

What can a personal Web page reveal about you? Many folks include the following personal info on their pages:

- email address
- real name
- home address, telephone number, other personal details
- work address, telephone number
- photos of self, home, pets, possessions
- list of possessions
- vacation dates, times the person will be out of town or away from home

Personal Web pages are fun, and a great way to share info with people who share similar interests. Be cautious, however, in publishing a page which advertises personal details that may be seen by a burglar, stalker, or other mischievous folk.

Warning signs of problems:	**What to do:**
Inquiries from your web page that show too much knowledge about you.	Report it to your network administrator, or to the postmaster at the offending party's email address. If you feel threatened, contact the police as well.
Inquiries that ask personal or inappropriate questions.	

Precautions to take:

Common sense posting
Common sense browsing

Steps you can take to protect yourself

Basic precautions:

- Common sense posting
- Common sense browsing

Extra security:

- Anonymous email names
- Anonymous remailers
- Encryption software
- Web security

Common sense posting

1. The safest policy is to not reveal any personal information on the Internet except your email address. If you want to make it easier for people to contact you by phone or snail mail, use your work phone and address.

- Don't give out personal info if you don't have to.
- Never give out your social security number, your birth date, or your mother's maiden name. These can be used to access your medical files, bank records, and government databases.
- Don't make public lists of your possessions.
- Be cautious when filling out online surveys.
- Don't send credit card card info over the Net in email, postings, or on the Web. Instead, call or snail mail payment information to the company. Consider using secure payment systems like First Virtual.

2. Protect your password. It is possible for someone to forge an email message with your name as the sender without knowing your password. It is also possible for someone to access your account with a found or stolen password, but much harder to prove.

   - Use good passwords.
   - Change your passwords regularly.
   - Don't give your passwords to anyone.
   - Don't let others use your account(s).
   - Don't store your password with your Internet software, such as in your POP email program, or your web browser.
   - Don't enter your password at suspicious prompts.

3. Be responsible with your account.

   - Check your usage history occasionally and make sure it corresponds to your actual usage. Contact your Internet provider to ask how to do this with your account.
   - Don't leave your email account open and unattended so that others may access it.
   - Don't send email from work that you wouldn't want your employer to see.

4. Be cautious of people you "meet" online. Take precautions if an Internet penpal wants to meet you in person.

   - Try to verify who the person is, where they live, and get their phone number.
   - Get to know each other on the phone before deciding to meet.
   - If you decide to meet in person, do so in a neutral public place.
   - If you decide to meet, try to bring a friend.
   - If you decide to meet, make sure others know about your meeting and what you know about your Internet friend.
   - Don't reveal where you live until you know this person well enough to safely invite them to your home.

- top of page -

Common sense browsing

In addition to common sense posting, the following should be observed when using a Web browser such as Netscape or Internet Explorer.

> "Because on today's Internet, people *do* know you are a dog..."

1. Be wary of your browser's history and cookie files. These files are usually designed to make a Web site easier to use. However, information that you may not wish to share can be stored in cookies and history files.

   - Don't browse inappropriate Web sites at work.Your browser's history and cookie files keep track of every site you visit.
   - Install a program to clear the cookie file, such as Cookie Monster for the Mac, and NSClean for Windows.
   - Use an "anonymizer" site to surf the web without revealing any personal information.
   - Don't use your Web browser for email. Your browser will "share" the email address stored in its preferences.

2. Be wary of hostile Java Applets.

   - Don't respond to requests for your login name and password while browsing. Hostile Java Applets can fool you with a false window asking for login info. Don't fall for it.

- Don't use Netscape version 2.0. Some of the security concerns recently reported in Java have been fixed in Netscape 2.01.

- top of page -

Extra Security

You may desire security beyond the basic rules of common sense. If you want a higher level of privacy, consider the following:

Consider using an anonymous email name

You do not have the right to impersonate someone else, or to commit fraudulent acts, but you do have the right to personal privacy and to anonymity.

Some people believe that unless you are a criminal there is no reason to use an anonymous name on the Internet. This is not true. Anonymity on the Net is much like having an unlisted phone number. Just as with a telephone account, the company who provides you with Internet service has the right to know your real name, but the rest of the world usually does not.

Your system administrator will need to know who you are. However, you may be allowed to choose whether your real name is accessible to other users. If not, ask your system administrator what your options are.

The state of Georgia recently passed a law (April 1996) which denies its citizens the right to an anonymous identity on the Internet. The Electronic Frontier Foundation and the American Civil Liberties Union believe this law is unconstitutional and unenforceable. See the EFF's files for more info on the lawsuit.

Consider using anonymous remailers

A remailer is a service which resends an email message or news posting to obscure the originator's name and email address. Some people use remailers routinely for email, but it is most often used for posting ads or responses in the personals section of Usenet newsgroups.

If you are interested in using a remailer, there are several references on the links page which will offer you the most up-to date info on which remailers are currently active for public use, and how remailers work (if you are interested).

Use remailers responsibly. The availability of remailers is not an excuse to commit harassment or other Internet abuse. A crime is still a crime even if you are anonymous.

Encryption software

Encryption software is a means of scrambling your email messages or other files so that they can only be read by someone who has a key to unscramble them. Encryption requires the use of public keys and private keys, and it can get pretty confusing for the average user.

PGP (Pretty Good Privacy) is the most common encryption software available. There are a few tutorials and guides available to make PGP a little easier to use and understand, but you might also consider a program which configures PGP for you from within your usual mail program. These are available for several platforms and may make encryption easier to use, although it is still not seamless.

Web security

The latest versions of Web browsers have incorporated encryption protocols called SSL (Secure Sockets Layer protocol) to enhance the security of transactions on the Web. Secure Sockets Layer protocol is used by Netscape to deliver server authentication, data encryption, and message integrity. You can read the latest information about this technology at Netscape's FAQ, On Security .

What to do if you have problems

- Gather your evidence
- Assess the damage
- Contact the user
- Contact online resources
- Contact offline resources

Gather your evidence

Whenever you have a problem with someone on the Net, try to save everything that might be useful in resolving the situation. Things that might be helpful include:

- Copies of email or other correspondence
- Posted articles
- Copies of Web pages
- Literature, warranties, receipts
- Record of relevant events with dates, times

- Email and posted articles include header information that may contain important clues to resolving your problem. However, your email program may not show all of the header info. You may need to change the configuration settings, or options, to see the "detailed" or "rich" header. Try to save that info if possible. Consult your system administrator on how to do this on your system.

Assess the damage

Before deciding what to do about the problem, assess the damages. Try to answer the following:

- What did you lose? (for example: money, data, time, reputation)
- Was your privacy violated?
- Was there any physical harm?
- Did you suffer harassment?
- What damage is possible if you do nothing about it?

The answers to these questions should help you decide whether to pursue a resolution. What will it cost to attempt resolution, compared to the cost of doing nothing?

Contact the user

The first and simplest approach is to be direct with the person you believe is causing your problem. It is possible there has been a miscommunication or technical problem. Sometimes the problem is not really being caused by the person you think is causing it (as in the case of spoofed email or a "hijacked" account broken into by a password sniffer). But in any case, they should made aware of the problem!

Contact online resources

If direct contact doesn't resolve your problem, there are a few folks to contact online:

- Your network administrator, or Internet service provider, should be able to help you with email and posting problems.
- If your Internet account is through work or school, your company or campus may have a security investigation group.
- Try contacting the other user's postmaster or system administrator, who can sometimes be reached at:
  postmaster@the.user's.domain
  (substitute the second part of the user's address for "the.user's.domain" in the above example)
- If the problem is with a mail list, report it to the person who mangages the list. They are usually reached at:
  listowner@the.list.address
  (substitute the second part of the list address for "the.list.address" in the above example)

Contact offline resources

Don't expect much from resources offline unless you have huge monetary losses. The Internet is confusing to local law enforcement and most governmental agencies. Many people in these offices do not know how to handle issues of harassment or computer crimes.

For local problems, check your phone directory for:

- Local law enforcement
- District attorney
- State attorney general

If the problem involves telephone "phreaking" or fraud over the telephone wires, contact:

- Your local telephone company
- The Federal Bureau of Investigation

If the problem involves snail mail contact:

- US Postal Service

For problems with transactions:

- The Better Business Bureau collects complaints against businesses.
- The Federal Trade Commission investigates transactions that cross state lines.

If you cannot resolve the problem with the above sources, you may need to consult an attorney. Make sure you choose one who is knowledgable about the Internet!

Caution: This page contains suggestions only and should not be substituted for legal advice.

Glossary of Security and Privacy Terms

This glossary does not attempt to include all terms related to the Web or Internet, but is intended to supplement the terminology used in this document. For a more general Internet glossary, try the Agtel Telecommunications Glossary, or the Glossary of Internet Terms.

anonymous remailers
Remailers are programs accessible on the Internet that route email and Usenet postings anonymously (i.e., the recipient cannot determine who sent the email or posted the article).
(See also: email and remailers)

chat groups, chat rooms

Chat groups are virtual meeting places where you can converse via keyboard with other people from all over the world. Unlike newsgroups or email, chat is "live." Internet Relay Chat is one form of chat service, but chat rooms also exist on subscriber services like America Online and CompuServe.
(See also Internet Relay Chat)

cracking

A malicious form of hacking.

email

Electronic **mail**. Messages, usually text, sent from one person to another through a computer. Email can be sent automatically to a large number of addresses (mailing list). (Yup, the word is now common enough that the hyphenated "e-mail" is no longer the correct spelling.)

email address

An email address is made up of two parts: name@domain

The part before the @ sign is your login ID.
Everything after the @ defines the computer where your account resides, otherwise known as the domain.

encryption software

Encryption is a method of scrambling a message so that it can only be read by a person who has key to unscramble it. Encryption software exists for email as well as World Wide Web browsing.
(see also PGP, SSL)

FAQ

Frequently Asked Questions. Documents that list answers to the most common questions on a particular subject. There are thousands of FAQs on subjects as different as personal finances and ostrich breeding . FAQs are generally written by people tired of answering the same question over and over.
(See also: All the FAQs)

finger

An Internet software program used to locate people on other Internet sites. Finger can also be used to access non-personal information. The most common use is to determine if a person has an account at a particular Internet site. To protect their users, many sites do not allow incoming Finger requests.

flame

A nasty email or newsgroup post that may invite an even nastier response.

hacker

A hacker is a person who is a computer guru, and who refrains from computer mischief. A computer guru who uses his or her knowledge of computers for mischief (or outright sabotage) is considered a cracker. Hackers usually command respect, crackers do not.

header

The area in an email message that contains information about who that message came from, when it was sent, etc.
(See also: email)

history file

Browsers like Netscape and Internet Explorer keep a record of every site you browse while on the web. This information is stored in the history file. Netscape names these files "Global History" on Macs, and "Netscape.hst" on PCs.
(See also: NSClean information)

IRC, Internet Relay Chat

A huge multi-user live chat area. There are a number major IRC servers around the world inked to each other. Anyone can create a "channel" and anything typed in a given channel is seen by all others on that channel. Private channels can (and are) created for multi-person "conference calls".
(see also chat group, IRC Undernet FAQs, IRC FAQs)

Java applet

A short piece of code written in Java, an object-oriented programming language designed for the WWW. Applets can spice up a Web page if they are used to display animations or form results. Applets can also be written to perform

"hostile" functions, such as rewriting your hard drive or stealing your login ID and password.
(See also: Hostile Applets, Java FAQ)

Listserv

The most widespread of mail lists, and sometimes used to refer to all mail lists. Listservs started on BITNET and are now common on the Internet.
(See also: email, mail list)

login ID, or login name

The account name used to access a computer system. Not secret (like a password.)
(See also: password)

MagicCookie

This is a file written to your hard drive when you use Netscape. The cookie file keeps track of info such as when you visit a Web site, where you're coming from, what kind of computer you have, and other details about your browsing habits.
(See also: history file, Web browsing tools)

mail list, mailing list

A (usually automated) system that allows an email to be sent to one address, then that message is copied and sent to all of the other subscribers to that particular mail list. Mail lists allow those with different kinds of email access to participate in discussions together.
(See also: email, Listserv, newsgroup)

network

When two or more computers are connected and sharing resources. Connect two or more networks together and you have an Internet. Connect computer networks all over the world and you have *the* Internet.

newsgroup

The name of discussion groups on Usenet. Newsgroups are like bulletin boards, whose messages can be read from any server in the world which subscribes to Usenet news.
(See also: mail list, Usenet)

packet switching

The technique used to move data around on the Internet. In packet switching, all the data coming from a computer is broken up into chunks, each chunk has the address of where it came from and where it is going. This allows chunks of data from many different sources to share the same transmission lines, and be sorted and directed to different routes by special machines along the way. This allows many people to use the same lines at the same time.
(See also: packet sniffing)

packet sniffing, snooping

Because packet switching is used to move data between computers on the Internet, computers can receive information that was intended for other machines. Capturing or intercepting information going over the network is called sniffing.

Sniffing email is relatively easy to perform and difficult to detect. Although it can be directed toward an individual machine or user, most sniffing is random and the chance of your email or other data being "snooped" is relatively small.
(see packet switching, Sniffer FAQ)

password

A (usually secret) code used to gain access to a locked system. Good passwords contain letters and non-letters and are not simple combinations such as: **Jan3**. A good password is a series of characters not found in a dictionary. A good password might be: **twbhtg3-5**. It could be remembered as **T**his **W**ould **B**e **H**ard **T**o **G**uess from **3** to **5**.
(See also: login)

PGP, Pretty Good Privacy

Pretty **G**ood **P**rivacy. A way of encrypting information sent through the Internet to secure privacy. Definitely better than no security at all, but a competent computer hacker or cracker could get through PGP.
(See also: encryption, hacker, cracker, encryption links)

phone phreaking

Phone phreaking is the phrase used for hacking or cracking a telephone network. Relevant to Internet security and privacy because some phreaking techniques can be used to intercept or "sniff" computer data.
(See also: hacker, packet sniffing)

post

To send a message to a newsgroup or a mailing list.
(See also: mailing list, newsgroup)

remailers

see anonymous remailers

signature file, sig file

A space that automatically includes several lines of text on an email or newsgroup post. These are easily created by the user and can include email address, snail mail address and phone numbers. Many times signatures will include graphics created with text characters.
(See also: email, newsgroup, snail mail, spam)

snail mail

Using the postal service to send information. It could take a few seconds to send an email across the globe. The same message sent through snail mail could take a week or longer.
(See also: email)

spam

Spamming is posting an email message (often an advertisement) to a large group of people, or to several newsgroups or listservs. Don't spam. It wastes computer resources and makes people angry. Spamming is grounds for your Internet provider to take away your email account, and will at least draw "flames" from recipients of your spam. (The name originates from a Monty Python spam skit.)
(See also: email, flame, Listserv, newsgroups)

spoofed mail

Email and newsgroup posts can be forged, or spoofed, when a user sends a message pretending to be someone else. Usually done as a joke, but spoofed mail can be destructive.
(See also: phoney-mail.txt , email and remailers)

SSL

Secure Sockets Layer protocol used by Netscape to deliver server authentication, data encryption, and message integrity. SSL is an attempt to ensure privacy on the WWW by transmitting data over the Internet in encrypted form.
(See also: On Security - Netscape FAQ)

Usenet

A world-wide network of discussion groups, with comments exchanged among hundreds of thousands of computers. Probably only half of Usenet groups are on the Internet, Usenet is completely decentralized, with over 10,000 discussion areas, called newsgroups .
(See also: newsgroup)

VeriSign ID

An attempt to authenticate and verify identity in Internet communications.
(See also: Digital ID from VeriSign)

Think different.

About this project

This document was written as a final project for a graduate course in Telecommunications, EIT 729, at the University of Georgia, Fall 1996.

It was inspired by the author's experiences in dealing with a cracker/stalker who not only made her life more interesting, but forced upon her a serious education in self protection, issues of privacy, and the inadequacies of the US legal system to deal with emerging technologies.

References

Bacard, A. (1995, March 27). Anonymous Remailer FAQ [Online FAQ]. Available: http://www.well.com/user/abacard/remail.html

Bacard, A. (1995, April 12). E-Mail Privacy FAQ [Online FAQ]. Available: http://www.well.com/user/abacard/email.html

Barrett, D. J. (1996). Bandits on the information superhighway. Cambridge, MA: O'Reilly and Associates.

December, J., & Ginsburg, M. (1995). HTML and CGI unleashed. Indianapolis, IN: Sams.net.

Hughes, L. J. (1995). Actually useful Internet security techniques. Indianapolis, Indiana: New Riders.

LaDue, M. D. (1996). Hostile applets on the horizon [Online article]. Available: http://cui.unige.ch/eao/www/Java/HostileArticle.html

Levine, J. R., Baroudi, C., & Young, M. L. (1995). The Internet for dummies. Cambridge, MA: IDG Books Worldwide.

Van Name, M. L., & Catchings, B. (1996, August 5). Have your cookies and beat them, too [Online serial article]. PC Week Online. Available: http://www.pcweek.com/opinion/0805/05cvn.html

Negrino, T. (1996). So what are browser cookies, anyway? [Online serial article]. MacWorld Online. Available: http://www.macworld.com/netsmart/

Rathbone, T. (1993). Modems for dummies. San Mateo, CA: IDG Books Worldwide.

Sterling, B. (1992). Hacker crackdown: Law and disorder on the electronic frontier. New York: Bantam.

Stoll, C. (1989). The cuckoo's egg: Tracking a spy through the maze of computer espionage. (1st ed.). New York: Doubleday.

Princeton Safe Internet Programming Team. (1996). Java Security: Frequently Asked Questions [Online FAQ]. Available: http://www.cs.princeton.edu/sip/java-faq.html.

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

ERIC®

REPRODUCTION RELEASE

(Specific Document)

I. DOCUMENT IDENTIFICATION:

Title:
Personal Security on the Internet

Author(s): Jan G. Hogle

Corporate Source:

Publication Date: December 1996

II. REPRODUCTION RELEASE:

In order to disseminate as widely as possible timely and significant materials of interest to the educational community, documents announced in the monthly abstract journal of the ERIC system, *Resources in Education* (RIE), are usually made available to users in microfiche, reproduced paper copy, and electronic media, and sold through the ERIC Document Reproduction Service (EDRS). Credit is given to the source of each document, and, if reproduction release is granted, one of the following notices is affixed to the document.

If permission is granted to reproduce and disseminate the identified document, please CHECK ONE of the following three options and sign at the bottom of the page.

The sample sticker shown below will be affixed to all Level 1 documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

1

Level 1

☑

Check here for Level 1 release, permitting reproduction and dissemination in microfiche or other ERIC archival media (e.g., electronic) *and* paper copy.

The sample sticker shown below will be affixed to all Level 2A documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE, AND IN ELECTRONIC MEDIA FOR ERIC COLLECTION SUBSCRIBERS ONLY, HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

2A

Level 2A

□

Check here for Level 2A release, permitting reproduction and dissemination in microfiche and in electronic media for ERIC archival collection subscribers only

The sample sticker shown below will be affixed to all Level 2B documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE ONLY HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

2B

Level 2B

□

Check here for Level 2B release, permitting reproduction and dissemination in microfiche only

Documents will be processed as indicated provided reproduction quality permits.
If permission to reproduce is granted, but no box is checked, documents will be processed at Level 1.

I hereby grant to the Educational Resources Information Center (ERIC) nonexclusive permission to reproduce and disseminate this document as indicated above. Reproduction from the ERIC microfiche or electronic media by persons other than ERIC employees and its system contractors requires permission from the copyright holder. Exception is made for non-profit reproduction by libraries and other service agencies to satisfy information needs of educators in response to discrete inquiries.

Sign here, → please

Signature: Hogle	Printed Name/Position/Title: Jan G. Hogle, PhD Candidate	
Organization/Address: University of Georgia, Athens, GA 30607	Telephone: 706-542-1351	FAX: 706-542-1827
	E-Mail Address: mocat@geocities.com	Date: Oct 30, 1998

(over)

III. DOCUMENT AVAILABILITY INFORMATION (FROM NON-ERIC SOURCE):

If permission to reproduce is not granted to ERIC, *or*, if you wish ERIC to cite the availability of the document from another source, please provide the following information regarding the availability of the document. (ERIC will not announce a document unless it is publicly available, and a dependable source can be specified. Contributors should also be aware that ERIC selection criteria are significantly more stringent for documents that cannot be made available through EDRS.)

Publisher/Distributor: ftp.twinpinefarm.com (author's web site)

Address: Available as a pdf file (persec.pdf) through anonymous ftp:
ftp://twinpinefarm.com/pub/pdf/

Price:
No fee.

IV. REFERRAL OF ERIC TO COPYRIGHT/REPRODUCTION RIGHTS HOLDER:

If the right to grant this reproduction release is held by someone other than the addressee, please provide the appropriate name and address:

Name:

Address:

V. WHERE TO SEND THIS FORM:

Send this form to the following ERIC Clearinghouse:

However, if solicited by the ERIC Facility, or if making an unsolicited contribution to ERIC, return this form (and the document being contributed) to:

ERIC Processing and Reference Facility
1100 West Street, 2nd Floor
Laurel, Maryland 20707-3598

Telephone: 301-497-4080
Toll Free: 800-799-3742
FAX: 301-953-0263
e-mail: ericfac@inet.ed.gov
WWW: http://ericfac.piccard.csc.com