Protecting yourself on the Internet

http://advosys.ca/tips/protect.html
Aug 02 2001

Introduction

Criminals and vandals are found on the Internet just like in real life. There isn't a higher proportion of scam artists and criminals on the Internet than you'd find walking in the downtown of any large city... it just seems that way.

Common sense help protect people on a busy downtown street. Most people know it's more dangerous to walk alone, more dangerous walking at night, and so on. However, on the Internet common sense has yet to be established and become "common sense".

We've all learned to be critical when encountering strangers on the sidewalk. We're naturally cautious around those we don't know. However, on the global sidewalk of the Internet, web sites, chat rooms, instant messaging and video−conferencing are new and often we aren't cautious enough. Most people are willing to trust flashy web sites, or strangers who are well spoken in a chat room even though they are still strangers, no different than someone who stops you on a street.

There are crackpots and dishonest people on the Internet, just are there are in real life. You'll encounter dishonest businesses too... companies who have no problem flood you with e−mail advertisements or violating your trust and privacy. Privacy, in particular, is the major concern on the Internet for individuals.

The trick is to become skeptical: stay aware and cautious about Internet web sites and people, just as you are in real life. This guide points out things to watch out for and ways to protect yourself personally on the Internet.

The people that you meet...

Millions of people interact every day on the Internet. Most of it is through e−mail and chat services like Instant Messenger and ICQ.

The power of print

Maybe it's human nature... but most of us give more substance to things we read than something we hear from a friend. If a telemarketer calls on the phone claiming you can lose 100 lbs for $25 just by popping a special pill, you'd be skeptical. You'd ask that telemarketer for proof, a free trial, and even after that you'd be skeptical about it.

Yet on the Internet when someone creates a professional web site with pictures and coordinated colors claiming the same thing, thousands of people send that company money without a second thought. After all,

if it's advertised on the Internet it must be legitimate, right?

The first rule of protecting yourself on the Internet: Don't believe everything you read. Be skeptical. Check it out before acting on any information.

This advice applies to *everything*, no matter what source: e−mail, web pages, and instant messaging. Treat web sites and every stranger you talk on the Internet as strangers... because that's really what they really are. Just because a product or service is presented on a fancy web site doesn't necessarily mean the claims are true.

Protecting your computer

If you download files, take precautions to prevent your computer being vandalized by a virus, trojan horse or worm.

Viruses and trojan horses

A "virus" is a small computer program someone wrote to hide itself inside another program. For example, a virus could be attached to a game downloaded from web site. Viruses don't normally disrupt the program they attach to, so you can down load an infected program and run it without knowing about it. Viruses stay hidden. Most are designed to copy themselves to other programs, "infecting" other programs on your computer or anything you share via floppy disk, mail or uploading.

At some time the virus will trigger, doing damage such as erasing your hard drive, sending mail to other users, or corrupting files. Most viruses only work on Windows computers, though some exist for Macintosh as well.

A "trojan horse" is similar. A trojan is a program that looks like one thing, such as a game or useful utility program, but really does something nasty, like erase your hard drive. Trojans are most common in e−mail messages. More than one person has opened an attached program that looked like a fun program only to watch it wipe their computer.

A "worm" is similar to a virus, except it exploits security problems in Microsoft Outlook or a other e−mail programs to automatically e−mail itself to others disguised as a harmless file attachment. When the recipient tries to view the attachment, the worm installs itself on their computer. If recipients also use Microsoft Outlook or another vulnerable e−mail program, the worm spreads further.

(Some "worms" also distribute themselves by exploiting flaws in Microsoft's web server product "Internet Information Server", but unless you also run a web site on Windows NT or Windows 2000 you should only need to be concerned with the e−mail form of Internet "worms").

If you use Microsoft Outlook or Outlook Express, any message you receive may contain a trojan or virus. Anyone stranger can exploit multiple design flaws in Outlook to trick them into destroying your computer or mailing copies of a virus to everyone in your address book. The "ILOVEYOU," "Melissa," and "SIRCAM" worms that exploited flaws in Microsoft's e−mail products victimized thousands of people.

If possible, use Eudora, Netscape Mail or any mail program other than Microsoft OutLook to read mail. If you're required to use Outlook, be sure your computer runs a scanner such as McAfee Viruscan or Norton AntiVirus. Scanners help to protect against known Outlook security problems, though they can't guard against recently discovered exploits.

Virus scanners

You can prevent damage from virus attacks in three ways:

- Use a virus scanner on your desktop computer.
- Avoid using Microsoft Outlook or Outlook Express for e−mail.
- Only download files from well known FTP and Web sites.
- Back up your computer regularly.

Virus scanners files for the signatures of known viruses. Most scanners also check e−mail attachments for hostile files. When a problem is found, the scanner can remove or delete the infected file. McAfee's ViruScan (http://www.mcafee.com/) or Symantec Antivirus make highly regarded virus scanners.

Reputable sites

Downloading from well−known FTP and web sites greatly reduces the chance of getting an infected file. Use the large shareware collections such as http://www.tucows.com or http://www.download.com which check files for known dangers and remove them if problems are found.

Regardless of where you download a file, always check it with a virus scanner. Checking a file for viruses after you open it is too late.

Backups are the best defense

Even if a virus does slip through your defenses, back up your computer regularly so you won't lose much information.

With a tape drive you can restore damaged files, or even rebuild your entire hard drive in a few hours. Tape backup drives are inexpensive these days− some cost only $150 or less... well worth the investment. Tape drives are also great for retrieving files you accidentally erase. Backups are the best way of preventing files on your computer from being lost. Many CR−RW (CD−ROM Read/Write) drives also come with simple backup software that let you back up your personal computer to a series of CD−ROMS.

Web browser holes

All web browsers, including Microsoft "Internet Explorer" and Netscape try to prevent security problems. However, security holes in all browsers are discovered frequently, especially with the Microsoft "Internet Explorer" browser. When a hole is discovered, a fix is usually made available from the manufacturer within a few days, but you have to actively check for updates often and install them.

To minimize the risk of an outsider using your web browser to gain access to your computer, keep your browser software up−to−date. The latest versions of the Microsoft and Netscape browsers have an option in the "Help" menu to check for updates and install them automatically. If you use Microsoft Windows, you may be able to update your computer automatically by visiting windowsupdate.com.

It's a good idea to update your computer once a month to check for new versions and updates.

One problem with these update features, however, is that vendors also use them to foist unwanted "extra" software on you, or completely replace your browser with the "latest" version. This is convenient when that's what you want, but usually it's best to wait a while before upgrading software. New versions of web browsers or extra software usually contain severe bugs. Extra software also increases download time, consumes disk

space, and most of it rarely needed.

When using an automatic upgrade feature, take time to read descriptions of what you're getting and uncheck items you don't want or aren't sure you need. While downloading a security fix for your browser, you may want to download a critical update to a newly discovered browser hole, but you can skip downloading an optional feature that displays oddball graphic types.

Protecting your privacy

Privacy is endangered on the Internet. Every time you visit a web site a record of the page you are viewing, your ISP's IP address, and the link you clicked on to get there are logged by the site you view. Some advertising banners also track your visit across multiple web sites, developing a profile of your personal interests. Your identity can then be revealed when you download a file, send e−mail or visit a chat room.

Anonymous Web access

All web sites collect visitor information. Most use it for ordinary usage statistics... times of day the site is most busy, which web pages are viewed the most, which type of web browsers are most popular. This information does not personally identify you.

However, wany web sites also send "cookies"... small information tags stored by your web browser. These are stored by your web browser and can through various tricks be used to identify you. Most often cookies are used by reputable web sites just to store your preferences, such as colors or layout info on a site that can be customized. Some commercial sites, however, exploit web browser cookies to identify you as an individual.

Cookies work as follows: a web site can ask your browser to store one line of text called a "cookie" on your hard drive. Usually only that same web site can get that information back... no other web site can see it, but the originating web site can use the cookie info to recognize your previous settings or customization options if they choose to. A cookie contains a very small amount of information, such as the date and time you last visited that web site, or an serial number the web server software uses to locate your previous information in a database.

Cookies can't reveal information you have not volunteered... they can only regurgitate information you've already given away. For example, you have to explicitly entered your name and e−mail address into a web form, a cookie could be used by that same web site to retrieve that information later.

Cookies became a threat to privacy when advertising companies such as Doubleclick embedded them in advertisements used on multiple web sites. Many of the ads you see at the top of web sites are provided by common advertising companies such as Doubleclick. Each time you visit a web site that displays an ad from a common advertiser, a cookie with a unique serial number is stored in your web browser. Ad companies use the serial number to track which web sites visited from that same browser.

The tracking history can be kept for years, recording every web site your browser visits that use the same advertiser. The advertisers sell this anonymous demographic information about your browsing traits. Once your interests are established from the history of web sites you visit, the demographic information can be used to customize ads on sites you visit to your interests and for other purposes.

Targeted ads and anonymous demographic information is not a large erosion of privacy. It can't identify you as an individual. However, if you ever enter your name or other personal information on a participating web site, the unique number the ad companies store in your browser can then be tied to you personally. For example, by answering a quick poll about your age group on a participating web site, the advertiser can add

that info to their profile database about you. Name, address, income and other information gathered anonymously on seemingly unrelated web sites can be tied to you if each site uses the same advertiser and the advertiser chooses to collect that info.

As long as you never type in personal information such your name to a participating web site, *and* the web sites never shares cookie IDs to an advertising agency such as doubleclick, your privacy remains within that one web site. Volunteering any personal information to a site that shares it with an advertiser can mean your identity is revealed to thousands of other web sites who also use that advertising agency.

If this bothers you, you can use a web anonymizer service such as Anonymizer to visit web sites. They stop cookies and other information used to track you. You might also want to check out JunkBuster, a free web browsing proxy that can filter cookies and other information from your web browser. Several other cookie control utilities can be downloaded from sites on the Internet to help you prune the tracking information many web sites store in your browser.

Free registration and personalization

Many web sites require you to "log in" to access their free services. For example, the New York Times requires a free registration before viewing most of their site. Other sites a "free registrations" so you can customize the site to your preference or access added services. Beware of this: if the web site does not have privacy policy that explicitly states your personal information will not be sold or used for any other purpose, it is likely your e−mail address and other personal info will be sold to advertisers.

In some cases, web sites that initially promised visitors their personal information would remain private forever turned around and sold that information when the business fell on hard times. Demographic information collected by web sites is valuable to marketeers and other businesses and is viewed as an asset held by the company. All company assets, even personal information you provided in confidence, are potential candidates for sale during hard times.

Again, an anonymizer service or cookie manager can help you remove unwanted tracking information from your web browser.

Anonymous mail and newsgroups

Your e−mail address is as personal as your telephone number. Unfortunately, just like your telephone number, advertisers want to know it and it can be abused. The most common e−mail abuse is junk mail... commonly called "spam". If you reveal your e−mail address by posting to chat forum, as a "mailto" on a web page or by volunteering it on a web form, you will probably soon start receiving hundreds of e−mail advertisements.

Illegal and illegitimate businesses are the majority of the junk e−mail advertisers. Dubious offers such as "Get rid of debt" and "find out anything about anyone" are usually advertisements by questionable companies who don't care that their ads are hostile and unwanted. They knowingly exploit loopholes in the Internet to send their unwanted advertisements.

Anonymous remailers are available to protect your identity. They let you send e−mail and post to newsgroups without revealing your name and e−mail address. People can still respond to you, but only through an anonymous account. To learn all about anonymous remailers and how to use them, check out Andre Bacard's Anonymous Remailer FAQ at http://www.andrebacard.com/remail.html.

> **Note:** If you chose to use an anonymous remailer, be sure to turn off your e−mail or news reader's signature feature before sending... it's no use posting anonymously if your messages

have a signature with your name and address at the bottom! Also, the anonymity provided by remailers have limits... don't try to use remailers for illegal or immoral activities. All anonymous remailers keep records of everything sent, and court orders can force those records to be revealed.

You can also use one of the many free web mail services such as Yahoo Mail to set up an anonymous e−mail account separate from your regular ISP mail address. Use the web mail address for subscriptions and to give out to strangers. If it becomes the target of spam, simple delete the account and sigh up for another.

For an interesting list of steps to protect your privacy, check out the Electronic Frontier Foundation's "Top 12 Ways to Protect Your Online Privacy" at http://www.eff.org/pub/Privacy/eff_privacy_top_12.html

Protecting confidentiality

The Internet is a great communication tool. However, the way the Net is designed also allows anyone with a little technical knowledge eavesdrop on information as it goes by. Every e−mail message, web page and newsgroup you read or send can potentially be captured and read by others.

The World Wide Postcard

Internet communications is about as confidential as a postcard. Don't send confidential information like credit card numbers, social insurance numbers, vacation plans, etc. across the Internet in e−mail or in a web page form without it being protected first.

For e−mail messages, a good way to protect confidentiality is with encryptions programs such as Pretty Good Privacy (PGP) or Gnu Privacy Guard (GPG) These utilities encrypt text and attachments so only the recipient can read it. If a message is intercepted, it cannot be read. PGP and GPG are a little complicated to use... but check your favourite download sites for front−ends available that simplify and integrate the utilities with your e−mail program. Both Eudora and MS Outlook have plug−ins that can automatically encrypt and decrypt mail.

PGP and GPG is also useful in protecting your identity. In addition to encrypting messages you can add a "digital signature" to prove the message was sent by you, not an impostor. A skilled person can forge headers in a mail message to make it appear the message came from you. Messages can also be tampered with enroute. Using a signature lets readers verify that it was indeed you who sent the message and the message was not tampered with.

For more information about confidentiality and protecting your identity on the Internet in general, see http://www.stack.nl/~galactus/remailers/.

Protecting your money

There are many web sites that sell items. You can buy things online just by filling out a form and entering your credit card number. However as explained above, Internet messages can be intercepted, which is bad news for credit card numbers.

Encrypted web sites

Many commercial web sites now use an encryption called "Secure Socket Layer" (SSL). SSL encrypts everything sent between you and the web site so outsiders can't intercept credit card or other information. The link also lets you verify the web site is who it says it is, not an imposter. All this is handled without any

special action from you... you see the web pages as before.

When connected to a secure site in Netscape, the small padlock or yellow key symbol at the lower left of the Netscape window will be unbroken. If you haven't turned it off, a message will also appear saying the site is secure. In Microsoft Internet Explorer, a padlock symbol appears at bottom of the Internet Explorer window you are connected to an encrypted web server. In all browsers, the URL of an encrypted site will begin 'https://' instead of the usual 'http://'.

What e−commerce doesn't want you to know

SSL (the scheme that encryptes in−transit information) doesn't guarentee your credit card number is safe. Far from it. SSL only does two things:

1. verifies the web site you're connected to is not an imposter
2. Stops outsiders from listening to the conversation between your web browser and the SSL web site

Contrary to industry hype, SSL does *not* guarantee your card number is safe. Once a web server receives your order via SSL, the credit card number is decrypted automatically. What the web site does with the number after that is entirely up to their programmers... they could print it out, store it in a diskette, or broadcast it on a billboard if they chose to.

Only the most diligent e−commerce web sites bother to re−encrypt your card number before they store it in their systems. Most often, your card number is kept *unencrypted* until your order has been processed by the company. Worse, many companies keep your card number even after they've processed your order, in case you make a later order. Obviously, such practices leave your card numbers ready to be salvaged by Internet thieves when they later break into that company's computers.

All exposures of credit card information from e−commerce sites have happened someone broke into a web server or Internet−connected database storing card numbers unencrypted. In *all known disclosures to date*, credit card information was obtained because of a server break−in, *not* because numbers were sniffed in−transit. SSL *only* protects against in−transit sniffing attacks... the least likely method outsiders use to obtain card numbers.

Despite the emphasis e−commerce sites place on SSL, it doesn't necessarily mean they also protect the information once they've it stored on their servers. Most e−commerce sites store card numbers on their servers unencrypted. Anyone who breaks into those servers can easily harvest your card numbers and other information. Many e−commerce sites even offer a "service" where they will keep your credit card number and personal info on file so you don't have to enter it again for future orders!

Before you place an order on a web site, check their ordering policy and terms. Ask about their policy regarding stolen card numbers... most will insist that can't happen because they use SSL, but you know better.

Credit card companies generally protect cardholders against fraudulent use beyond $50.00 of unauthorized use... ask if the e−commerce site you are dealing with has a policy of reimbursing the $50.00 if your number gets stolen from their servers. Most don't, and they won't until consumers demand they treat card numbers more responsibly.

NEVER allow a web site to keep your card number on file... it's bad enough that most sites store orders−in−progress and transaction histories in unencrypted form... allowing your card number to remain on file in their systems for months is asking for trouble. Protecting yourself is well worth the inconvenience of having to input your card number and address each time you place an order.

For more information about encrypted web sites and SSL, see
http://home.netscape.com/info/security−doc.html

Shopping on the Internet

Never send credit card information across the Internet unless you use a web sites that uses SSL or other encryption programs like PGP or GPG. See above for other tips regarding SSL web sites. Even with these precautions, however, shopping on the Internet should be treated the same as shopping by mail or ordering by phone: get the company's mailing address and telephone numbers so you can contact them if there are problems, and deal only with reputable companies.

Before shopping on the Internet, check out The Public Eye at http://www.thepubliceye.com/ for tips and ratings of various on−line retailers.

Several online shopping helpful tips are also available from the Better Business Bureau Online at http://www.bbb.org/.

Conclusion

The Internet isn't more threatening than real life, as long as you stay alert. There are no more scams, crackpots and criminals on the Internet than in ordinary society. Be sceptical, and the take precautions mentioned above:

- Don't believe everything you hear or assume the speaker is who they say they are.
- A fancy looking web site is not necessarily legitimate.
- Use a virus scanner and only download files from reputable sites.
- Back up your computer regularly. Tape drives are cheap.
- Keep your web browser software up−to−date.
- You can obscure your identity by using web anonymizers and anonymous remailers.
- Encrypt confidential messages using Pretty Good Privacy (PGP) or GNU Privacy Guard (GPG).
- PGP and GPG can "sign" messages to prove you really wrote them and to avoid tampering.
- Only use SSL web connections when buying on the Internet and do not let the site store your card information.
- Treat Internet shopping like mail order or phone shopping: deal only with reputable companies and ask about their policy regarding stolen card numbers.

Comments, suggestions, criticisms, additions to this document?
Please e−mail tips@advosys.ca

Latest version of this document available at http://advosys.ca/tips/protect.html

Last modified Aug 02 2001

Copyright and terms of use

Use of this document

Permission to use this document from the Advosys Consulting web site is granted, provided that (1) This notice notice appears in all copies, (2) use is for informational and non−commercial or personal use only and will not be copied, reprinted, or posted on any network, computer or broadcast in any media, and (3) no modifications of the document are made.

Educational institutions (specifically K−12, universities and community colleges) may reproduce the Documents for distribution in the classroom, provided that (1) the below copyright notice appears on all copies, and (2) the original Uniform Resource Locator ("URL") of the document on the Advosys Consulting web site appears on all copies.

Use of this document for any other purpose requires written permission of Advosys Consulting Inc.

Limitation of liability

Advosys Consulting take no responsibility for the accuracy or validity of any claims or statements contained in the Documents and related graphics ("the content") on the Advosys web site. Further, Advosys Consulting Inc. makes no representations about the suitability of any of the information contained in the content for any purpose. All such documents, related graphics, products and services are provided "as is" and without warranties or conditions of any kind. In no event shall Advosys Consulting Inc. be liable for any damages whatsoever, including special, indirect or consequential damages, arising out of or in connection with the use or performance of information, products or services available on or through the Advosys Site.

Trademarks

Product, brand and company names and logos used on the Advosys web site site are the property of their respective owners.

About Advosys Consulting

Advosys Consulting is a privately held systems management corporation. Our global headquarters is in Ottawa, Ontario Canada. Formerly known as "Webber Technical Services", we have been providing systems management, computer engineering, security and consulting to private sector and government clients since 1991.

Areas of expertise

Advosys is a diversified consulting firm providing services in many areas of Information technology:

- Internet technologies
- Firewalls and information security
- Web applications
- Network architecture
- Unix and Linux systems management

Unbiased recommendations

Advosys Consulting is an *independent* consulting firm. We have broad experience with multiple vendors including Sun, Hewlett−Packard and Microsoft but are not a reseller of their hardware or software.

Unlike many consulting firms, Advosys receives no commissions, percentages, or other rewards from companies for promoting particular products or services.

This allows us the freedom to offer uncompromised objectivity. We have knowledge and experience with a broad range of products and technologies and can recommend solutions from any manufacturer, or open−source freeware if that is what best fits the requirements. Advosys works only for you, our client, not for a product manufacturer.

For more information, please visit us at http://advosys.ca