



The University Commons Personal Computer Security Policy

The University Commons Data Network

The security of our computer network begins at home, with each of our residents. Unfortunately, keeping your computers safe, particularly while connected to the Internet, has become an unwelcome do-it-yourself project. Neither Microsoft nor Apple can do it for you.

The purpose of these recommendations is to assist you to protect your expenditure on computing resources, protect your personal information from loss or corruption, and help you to be alert you to the risks of fraud posed by the Internet.

INDEX

1 LOGICAL SECURITY	3
<u>MALWARE</u>	3
<u>Viruses</u>	3
<u>Trojans</u>	5
<u>Spyware</u>	5
<u>OTHER TOPICS FOR CONCERN</u>	6
<u>Adware</u>	6
<u>Spam</u>	7
<u>Probes</u>	7
<u>Wireless Connectivity</u>	8
<u>Phishing</u>	8
<u>Hoaxes and Myths</u>	9
<u>Hard Drive Clutter</u>	9
<u>Hard Disc Failure (crashes)</u>	10
<u>Data Loss</u>	11
<u>Critical Computer Information</u>	11
<u>Guest Users</u>	12

<u>COMMONSENSE STEPS TO PROTECT YOURSELF</u>	12
2 <u>PHYSICAL SECURITY</u>	13
<i><u>Security Protections</u></i>	13
3 <u>INTERNET FRAUD</u>	14
4 <u>TELEPHONE FRAUD</u>	16
5 <u>HOW TO SECTION</u>	17
<i><u>Website address for program downloads</u></i>	17
<i><u>How to download programs</u></i>	17
<i><u>How to set space parameter for System Restore</u></i>	17
<i><u>How to set space parameter for Outlook Express</u></i>	17
<i><u>How to remove unneeded programs</u></i>	18
<i><u>How to declutter memory</u></i>	18
<i><u>How to update Windows</u></i>	18
<i><u>How to run CHKDSK, Disk Cleanup and Defrag</u></i>	18
<i><u>How to save device drivers</u></i>	18
6 <u>GLOSSARY</u>	19

The University Commons Personal Computer Security Policy

1 Logical Security

Logical security is the protection of the information on your hard disk, both software programs and the records (files) you have created yourself. (In computer-speak, logical implies a broader view than the physical, which is your hard drive, your monitor and other physical accouterments connected to your computer.)

Malware

Internet Security has become a very important aspect for everyone who uses the Internet, whether it is for work, play, education or a mixture of all three. Internet security issues include: viruses, trojans, key loggers, spyware, and others. These are commonly known as Malware. What is malware? Software that invades your computer, usually with malicious intent to do damage to your computer, other people's computers and the Internet itself. It can take control of your computer, corrupt your computer files, steal your passwords, steal your bank or credit account and then spread itself to other computers.

You're at risk whenever you're connected to the Internet, when you open your e-mail, or when you open an unscanned removable disc, such as a CD or floppy, or a zip drive. Fortunately, there are a number of ways of combating these security problems.

Viruses

The most widespread threat is that presented by so-called "viruses." What is a virus? Malicious computer code that attaches itself to your programs, documents or system files. It makes copies of itself, sending itself to addresses in your address book, spreading across computers and networks. Most viruses are spread through infected e-mail attachments, instant messaging or downloaded software, such as games or screensavers. But macro-viruses spread via the exchange of infected removable discs.

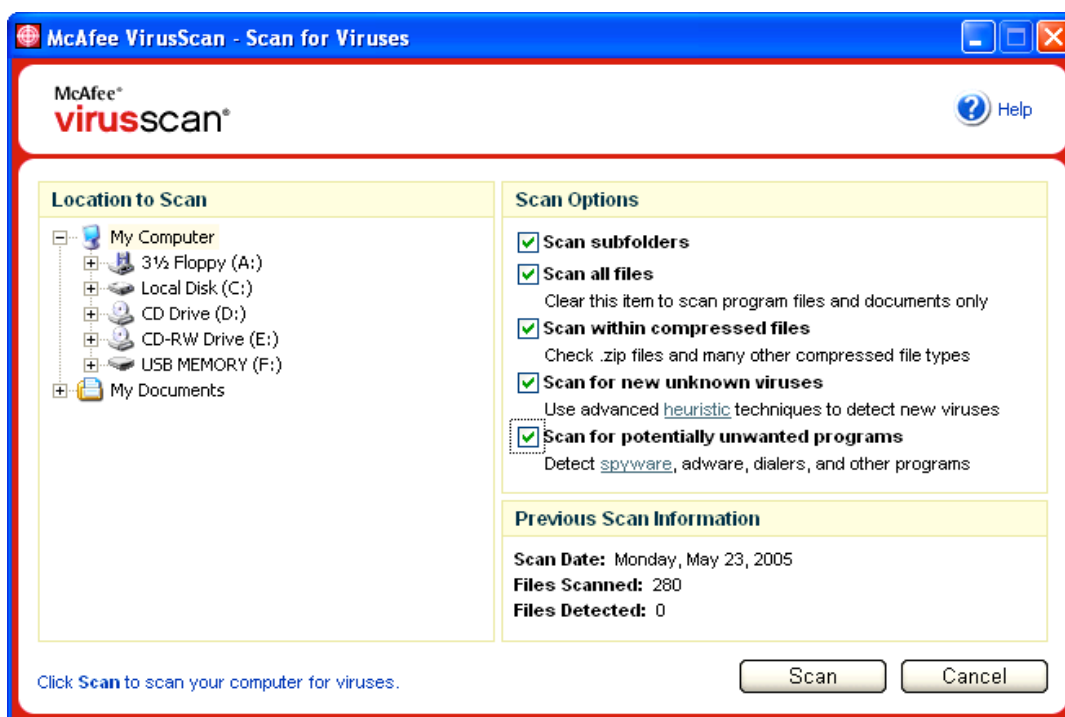
Protection: Two actions you can take to protect yourself against this are:

- Install and automatically update antivirus software
- Download and keep current the operating system patches made available by the manufacturer of your software system

Antivirus software. Leading vendors of this are McAfee and Norton, comprising about 95% of the retail market. (Subscribers to the U of M e-mail service are provided with McAfee.) It is essential to register the product with the manufacturer so it can be activated and you can receive and install automatic updates. New

threats are identified on a daily basis, and your software must be kept up to date. Licenses are usually good for twelve months and must be renewed when they expire. This can be done online. The package warns you of pending expiration, and invites you to renew. (Some viruses block the installation and/or updating of antivirus software, so don't wait until your computer is infected to purchase and install an antivirus program.)

While the antivirus software is actively protecting your machine in the background while you are using it, you should also periodically carry out a complete **scan** of your hard disk to check if anything has slipped through the protective barrier. The illustration below is for McAfee.

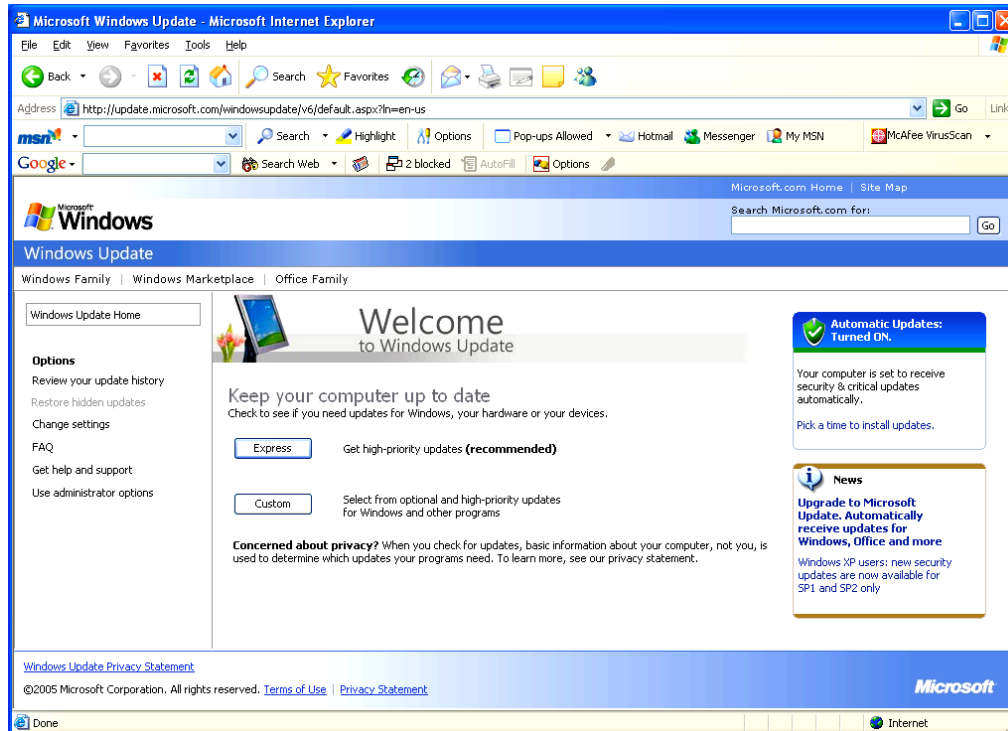


Security patches. Patches are pieces of code that correct vulnerabilities in the software of your operating system that create a risk of being exploited by hackers.

Protection: How you do this will depend on your operating system; a personal computer can be set up to receive such patches automatically.

For OS X: System Preferences>System>Software Update

For Microsoft: Microsoft Windows Update is illustrated below. It is accessed via the Control Panel. (For Windows, these tend to arrive in multiples, as Microsoft is the favorite target for the writers of hacker code.)



Trojans

What is a trojan? A program that does more than depicted, like the Trojan horse for which it is named. It may appear to be a cute screensaver or a neat game, but when installed it can corrupt or destroy files, disable hardware or open back doors into your computer so hackers can gain access while you're on the Internet and take over your computer.

Trojan protection: a scanner that recognizes trojans, for example:

Trojanscan (free download) www.trojanscan.com (and like any scanner, it must be kept current with latest definitions). Scan e-mail and attachments, files on hard drive, DVDs, CDs, floppies, etc.

Spyware

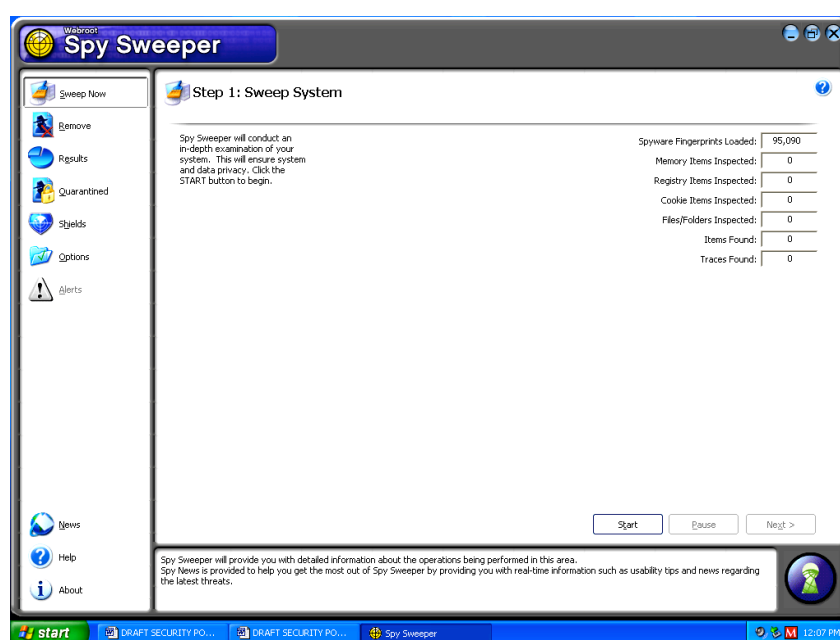
What is spyware? Instances of programming code often referred to as "cookies," put into your computer, usually without your knowledge, that allow access from the Internet. Some can serve beneficial purposes, such as allowing a manufacturer to recognize that you are a licensed user, thereby enabling you to get updates to your software. Tax software is a good example of this.

However, in most cases, spyware programs are not innocent; they open up your computer to unwanted interventions and may be designed, for example, to reveal private passwords. So-called "free" software is often the bait to induce you to load

concealed and unwanted spyware. An overload of spyware can seriously compromise the performance of your computer's operating system by taking up memory.

Anti-spyware products. Anti-spyware products function in a way similar to antivirus products in that they contain a library of undesirable pieces of computer code. Using these as a reference they stop these code definitions from being installed on your computer. There are a number of vendors, such as Spybot and Spy Sweeper.

As with antivirus software you need to keep the license current and accept regular updates. Periodic scans should be carried out. The Webroot product is illustrated below, showing at the date when this document was prepared, some 95,000 items in its database.



Other Topics for Concern

Adware

What is adware? Computer programs that pop up ads in your face. They are downloaded along with Web pages to monitor your browsing habits and individual preferences, or they can be downloaded as free programs to provide a service, e.g., Gator (currently a.k.a. Claria), Weatherbug.

Adware protection: A scanning program that recognizes adware, for example:

- Ad-Aware is a free pop-up blocker
- The Google toolbar has a downloadable pop-up blocker available for Internet Explorer
- Macintosh's Safari has a toggle on the Menu Bar; check "block pop-up windows"

Spam

What is spam? Unsolicited, disruptive junk e-mail. Two out of three "spam" e-mail messages contain false information of some sort, according to an analysis of unsolicited e-mail pitches collected by the FTC. Some e-mail providers have anti-spam filters built in as part of the service, MSN, for example.

Spam protection: An anti-spam filter, for example:

- Set up Outlook Express to filter messages with known characteristics
- Train Mac Mail to recognize spam (found under the Menu Bar; uses Boolean logic to train)
- Purchase McAfee's Spam Killer, Mailwasher, SpamCop, or Spam Alert

Probes

What are probes? Computers that send pings (inquiries) to find open ports in unprotected computers, with the intent to send in trojans, worms, or key loggers in order to take over your computer remotely and turn it into a robot for their use.

Probe protection: Firewall

What is a firewall? A firewall most frequently refers to a dedicated computer placed between the outside world and a local network. It contains a set of rules regarding what types of data it will let through. University Commons has such a firewall protecting our "always on" connection. (Prior to its installation, the UC was subject to a constant bombardment, mainly from academic sources.)

Firewalls—software or hardware. ZoneAlarm is available as a free download. Black Ice, Norton and McAfee software products may be purchased. Hardware routers also act as firewalls. At a minimum, the firewalls that come built in with Windows and Macintosh X operating systems should be activated, although they do not provide as much protection as the ones listed above.

Windows: Start>Control Panel>Windows Firewall>On>Exceptions tab; uncheck file & printer sharing and remote desktop

OS X: System Preferences>System>Firewall tab; click on

However, there are some qualifiers. Our firewall protects us from outside intrusion. It does not protect us from errors of security omission and commission inside our UC *domain*, as it is called, though this should not be viewed as a serious potential hazard for us.

Another qualifier is that anybody using wireless technology is not protected by our network firewall from intrusion; such users need to take their own precautions. See below under wireless connectivity.

Probably the biggest risk exposure comes from laptop computers that are taken offsite and then brought back to UC.

Mobile laptops need to have proper software firewalls installed on an individual basis. Five minutes plugged into a hotel broadband connection is sufficient to prove the point. Do not rely on the strength of the built-in firewall that comes with the latest versions of Windows. (See next section, below.)

Wireless Connectivity

With a hand-held computer, a wireless card, and a software program like Kismet (downloadable free and legal), anyone can drive around and locate wireless networks in offices and residences nearby. Left untended, the wireless technology that can quickly connect your computers and printers will also literally broadcast every bit of your transmitted information to the drive-by hacker: usernames, passwords, credit card numbers and other confidential information. Wireless networks can be set up to encrypt the text being sent, but few bother to do this.

Solution:

- For ease of installation most packages come with the security system switched off by default; follow the manufacturer's instructions and switch on the security settings
- Install robust firewall and virus protections as described above
- Disable file- and printer-sharing functions as these constitute a backdoor into your computer

For XP: Start>Control Panel>Windows Firewall>Exceptions tab; uncheck the box next to File and Printer Sharing

In Mac OS X: System Preferences>Sharing>Services; uncheck boxes

For additional advice:

- Visit Microsoft.com/atwork/stayconnected/hotspots.mspx
- Visit Apple.com/support

Phishing

What is phishing? Use of rogue e-mails and fraudulent Web sites designed to fool recipients into divulging personal financial data, credit card numbers, account usernames and passwords, social security numbers—any kind of valuable personal information. These e-mail letterheads closely resemble the trusted logos of well-known banks, online retailers, credit card companies and computer giants to get you to bite.

The Gartner Group estimates that some 7M victims have been affected as at the date of the compilation of this document.

Protection against phishing:

- Do not answer suspicious e-mails; look at URLs carefully for validity
- Call the real sender/website owner for verification of request; most legitimate companies DO NOT use these techniques
- There are a number of commercial products on the market: Clear Search from phishing.net; FraudEliminatorPro is a toolbar for Internet Explorer and Firefox; a free download is TrustToolbar which is a plug in for Internet Explorer

Hoaxes and Myths

Some consider these hoaxes to be “mind viruses.” Forwarded endlessly via e-mail, they clog mailboxes and waste productivity. A few hoaxes can cause serious damage, for example, those that trick computer users into removing essential files from their computers.

Protection against hoaxes and myths:

Check the following Web sites before following directions in an e-mail:

- www.vmyths.com
- <http://hoaxbusters.ciac.org>
- <http://urbanlegends.about.com/b/archives.htm>
- www.symantec.com/avcdnter/hoax.html
- virusbusters.its.umich.edu/; click on Hoaxes, Hooey and Hogwash

Hard Drive Clutter

What is clutter? Your hard drive can fill up with all kinds of clutter: programs you no longer use, outdated programs, excessive System Restore points, too many temporary files, duplicate files (pictures, music, documents). All this clutter slows down the operation of your hard drive, and it also slows down virus, spyware and adware scans.

Solution—Windows:

Microsoft provides a fairly simple tool called Disk Cleanup: click on Start>All Programs>Accessories>System Tools>Disk Cleanup (you can run it from there)

Windows users may want to make this tool more accessible: right-click on the Disk Cleanup icon (a dropdown menu will appear); click on Create Shortcut (a Disk Cleanup [2] icon will appear); hold down the left key and drag it onto your desktop screen (run it from time to time)

There are commercial products that do a more thorough job—Norton SystemWorks' One Button Checkup, Webroot's WindowWasher, McAfee's QuickClean—but these have to be purchased and installed separately.

Other solutions to consider:

Windows:

- Set space allocations to reasonable values
 - Temporary Internet files—1 to 5 MB
 - System Restore space—1 GB
 - Remove temporary Internet files
- Use Space Odyssey to remove excessive files
- Manage Windows parameters—change parameters for Windows components
 - Start menu; control panel entries
 - Use TWEAK UI from Microsoft to change the parameters

Mac OS X: Disk Utility>First Aid>Repair Disk Permissions

Both—

- Remove unneeded programs
- Clean out temporary files, downloaded programs
- Check your e-mail trashcan, "sent" mailbox, junk mailbox
- Check your Web browser's cache (Safari's Reset command clears History, empties Cache, clears Downloads and removes all Cookies in one sweep)

Hard Disc Failure (crashes)

Protect your hard drive from crashes.

Solution—

- Windows: Run CHKDSK and Defrag programs
- Clean out invalid shortcuts, program links, etc.
- Use Norton SystemWorks or WinDoctor (programs that fix a host of registry problems)
- Download and run Registry Cleaner Programs

Windows has a simple defragmentation tool called Disk Defragmenter. Click on Start>All Programs>Accessories>System Tools>Disk Defragmenter. You can run it from there. To put it on the PC's desktop follow the steps described under Disk Cleanup.

Note: ToniArts Easy Cleaner—a free program that provides a number of useful PC maintenance functions including the removal of invalid entries from your Windows registry, the identification and removal of duplicate and other un-needed files, and the option of cleaning up your start menu. (Not, however, for the novice.)

Data Loss

To protect yourself against data loss because of a computer crash or unintentional deleting of needed files, you need to make regular backups.

Solution:

Make backup easy. What to back up:

- My Documents, My Pictures, My Music
- Favorites or Bookmarks
- Address Book and E-mail
- Other personal files (e.g., Quicken or Money)
- Device drivers (programs that communicate to hardware devices)

Create a folder structure within My Documents: My Spreadsheets, My Letters, My Records, etc. Within these folders make category subfolders. Put all files in the folders and subfolders. Record My Documents on CD or DVD on a regular basis.

Critical Computer Information

Protect yourself against loss of passwords, user IDs and product keys.

Problems:

Password protection. Passwords can be described under the following headings:

- The most boring topic in computer technology
- The most neglected and taken for granted
- The easiest way to compromise a computer
- One of the most essential first lines of defense

The user is supposed to remember them all and not write them down. An active user can have scores of usernames and passwords so this advice is not always practical.

Solutions:

One can start by not having a not-so-obvious username as a first line of defense, particularly if conducting online banking or accessing a credit card account. Instead of say, bradtjones, try worry76wort. The password itself should be alphanumeric and mixed upper and lower case: prZ98hTlp. Write them down and keep them safe from prying eyes. Avoid Post-It notes stuck to the monitor. Password lock boxes can be installed on your computer or your PDA (personal digital assistant, e.g., Palm Pilot, Blackberry).

Purchased password managers include:

- Dataviz Passwords Plus for Palm
- Norton Password Manager for PCs

Note: All of the above recommendations also apply to keeping PIN numbers secure.

Product key protection: Use Belarc Advisor to save your information.

Other computer requisites:

Practice safe storage of your vital computer information. (Also see under Storage.)

Guest Users

Most of you will be familiar with the commercial showing a company's system being compromised during Bring Your Daughter to Work Day. The child downloads some "cool software," etc. To avoid such cosmic events happening to you, you should set up restricted Guest Accounts for visiting descendants.

Solution:

Windows: Start>Control Panel>User Accounts>Guest

Mac OS X: System Preferences>System>Accounts>New User. Fill in name, password, other information (to shield your computer further, limit the guest's capabilities, i.e., permissions)

Commonsense Steps To Protect Yourself

The odds are that hackers will continue to find unique ways of spreading their destructive wares. Protect yourself:

- Make regular backups of your data files
- Don't use files from others without scanning them, and keep your scan software current
- Download all security patches
- Create a system inventory, with date and source of program; enter updates (this is an indispensable aid for vendor support or UC mentor support)
- Beware hoaxes, especially those that tell you to make changes to your computer
- Show file extensions for all files
- Hide Preview Pane in e-mail program (in Outlook Express: View>Layout and uncheck "Show Preview Pane")
- Turn off your computer when you are finished for the day (Windows XP users can logically disconnect from the network when they are not actively using it)
- Disconnect the Ethernet network cable from the wall outlet when not in use
- Avoid using the computer during major electrical storms as incoming power and utility lines are vulnerable

2 Physical Security

Physical security consists of the protection of your equipment, archived material and software disks.

Security Protections

Surge protection. This is a device that protects the circuitry of your computer from spikes in the power supply. In addition to your computer and peripheral devices they can also protect the phone line. (An Ethernet cable slot is not normally available in consumer models.)

It is also sensible to switch off your computer during an electrical storm as the public power grid may be vulnerable to power outages. Commercial enterprises invest in an uninterruptible power supply (UPS). This is a battery reserve that allows the computer to be shut down in an orderly manner without losing data. Small devices are available for the private or small-business user for under \$100. (See Office Max or other supply outlets.)

Dust. Dust accumulates between the keys of keyboard and in the moving parts of a printer. This can be blown free by means of a compressed gas canister, readily available from office supply stores.

Spillages. Avoid spillages as the contacts under the keyboard keys can be damaged by spills from coffee or soda.

Cables. Spaghetti-like cable tangles can be corralled by wrap-around spiral devices or cable caddies. This may also prevent a trip and fall.

Backups. In a professional environment, considerable attention is given to making back-ups of the contents of directories. In a private setting it is a matter of preference and taste. If your computer is equipped with a CD burner, it is a simple task periodically to click on the My Documents directory (folder on Mac) and copy it to a CD or DVD disk. Consider this for important personal files.

Some commercial applications may include a feature where your information is backed up to the software manufacturer's server as an additional precaution.

Storage. Program disks, software product keys, proofs of purchase and manuals should be organized and stored in a safe place. If software is purchased and downloaded over the Internet, ensure that the invoice and product key information is printed out and filed.

Without the software disks it is difficult, if not impossible, to restore a damaged or corrupted application. This is especially so of printer drivers, which tend to be very device specific.

3 Internet Fraud

The Internet provides golden opportunities to fraudsters. Their methods have been given such terms as “phishing,” “pharming” and “typosquatting.” They have one aim in common—to part you from your money. This is done indirectly by trying to persuade you to provide bank details and passwords on the pretense that your financial institution is checking its records. The e-mails and linked websites tend to look like the real thing, but poor spelling and poor grammar are often a giveaway. Also look carefully at the Web address to which you have been directed.

This topic and some software solutions are discussed above, but good old-fashioned suspicion is the best protection. The following recommendations are provided by the SANS Institute, an industry leader in IT security.

1. The most common form of phishing is by e-mail (banks do not seek information using this method)
2. Don't click on the link in an e-mail that asks for your personal information
3. Phishing can also happen by phone via automatic dialers (if in doubt terminate the call and call back on the regular 1-800 number provided by your financial institution)
4. If someone contacts you and says you've been a victim of fraud, verify the person's identity before you provide any personal information
5. Be suspicious if someone contacts you unexpectedly and asks for your personal information
6. Act immediately if you've been hooked by a phisher
7. Even if you didn't get hooked, report phishing

Here are some recommendations from Microsoft's website:
“What To Do If You're a Victim of Fraud” (pub. Nov. 4, 2004)

“The Internet can be a great place to communicate with friends and family, play games, and shop. Unfortunately, all of those activities can leave you vulnerable to online fraud. You can do your best to prevent phishing attacks on your identity, avoid spyware and other unwanted software, ignore e-mail hoaxes promising easy money, and shop more safely online, but no method or system can guarantee total safety and security.¹

“If you think you've been scammed, immediately follow these steps. The faster you contact the proper authorities, the more likely you are to minimize the damage a scammer can do to your identity, your credit, and your bank account.

¹ This is especially true of data stolen from the servers of a credit-card service provider; federal law is weak in this area.

“File a report with your local police department. Get a copy of the police report to notify your bank, credit card company, and other creditors that you are a victim of a crime, not a credit abuser. Depending on where you live, you may be required to file a report in the jurisdiction where the crime actually took place.

“Place a fraud alert on your credit reports. Ask that no new credit be granted without your approval. Review your reports carefully; look for things like inquiries you didn't initiate, accounts you didn't open, and unexplained debts. In the United States, you can contact these three credit bureaus:

Equifax (800) 525-6285
Experian (888) 397-3742
TransUnion (800) 680-7289

“Outside the United States, you can contact your bank or financial institution, who can direct you to the relevant organization or agency.

“Close any fraudulently accessed or opened accounts. Speak with the security or fraud department of each bank or financial institution you deal with, including credit card companies, and follow up with a letter.

“Contact the genuine company or organization if you believe you've given sensitive information to an unknown source masquerading as that real company or organization. This is known as a phishing attack. If you contact the real company immediately, they may be able to lessen the damage to you and others.

“Change the passwords on *all* of your online accounts, starting with any that are related to financial institutions or information.

“In the United States, file a complaint with the Federal Trade Commission (FTC). If you are a victim of any type of identity theft, you can report the theft by calling the FTC's toll-free Identity Theft Hotline at (877) ID-THEFT or (877) 438-4338. You can also file a complaint online.

“Counselors will advise you on how to deal with the credit-related problems that could result from identity theft.

“Tip: Download and print the FTC's Identity Theft affidavit (the format is Adobe Portable Document Format or .pdf). Fill it out and send it to credit card agencies to help minimize your responsibility for any debts incurred by those who stole your identity.

“In the United States, report the fraud to Fraud.org, the National Fraud Information Center. Use the online complaint form or call (800) 876-7060.

“Record and save everything you do to clear up the wrongdoing, including copies of e-mail messages, written correspondence, and records of telephone calls.”

4 Telephone Fraud

Some telephone practices we need to be aware of:

Slamming is the practice of changing your long distance carrier without your knowledge or permission. This practice by competing carriers is both illegal and widespread notwithstanding the FCC's slamming liability rules. It can be prevented by asking your local phone company to put a "pick-freeze" on your choice of long distance provider.

Cramming is the practice of placing unauthorized, deceptive or misleading charges on phone bills. The FCC makes the following recommendations:

1. Review your phone bill every month. Read each line and make sure you know the names of the companies listed. Double-check that their rates are what you were told originally. Also, make sure there are not charges for calls you didn't make or services you didn't authorize.
2. If a description of a service on your bill is unclear call the company that charged you and ask them to explain it. Before you sign up for any kind of telephone or Internet service, read all of the forms and promotional information available. Don't overlook the fine print on any material.
3. Finally, use your power as a consumer to get the best deal possible. If you think you are being charged incorrectly, start shopping for a better service provider.

If you think you have been crammed you should call the company that charged you and ask for an explanation. If the charges are unauthorized ask for an adjustment. Then call and report the charges to your local phone company and then ask how to remove these charges from your bill.

If you still can't get the matter resolved you should file a written complaint with the FCC. Most complaints are resolved prior to this because the FCC has the power to levy heavy fines on the company placing unauthorized charges.

Send your written complaint(s) to:

FCC
Common Carrier Bureau
Consumer Complaints
Mail Stop Code 1066A2
Washington, D.C. 20554

5 How To Section

Website address for program downloads

Belarc Advisor: www.belarc.com

Spybot: www.PCWorld.com (search site for spybot search & destroy 1.3)

Tweak UI: www.microsoft.com (under PowerToys for XP page)

Ad-Aware: www.lavasoft.com

Win Patrol 8.1: www.winpatrol.com

ZoneAlarm: www.zonelabs.com

Space Odyssey: www.PCWorld.com (search site for space odyssey v2.0)

Easy Cleaner: <http://personal.inet.fi/business/toniarts/>

How to download programs

Windows—

For a particular program you want:

Type name into Google to find site

Type site address into address space & click GO

On site look for downloads or free download

On next window look for Download here

or a program name ending in .exe

Double-click and when asked save to desktop (this is the installer file)

Double-click installer file icon to install the program and follow the Wizard instructions (when completed, you can now send installer to the recycle bin)

OS X—When downloading software, several new icons will appear on the Desktop. (Usually these will be dragged to Trash after installation.) If a folder appears, it must be opened to reach the application. If a file icon with .pkg or .mpkg appears, the Apple Installer will provide a guide to installation. Or a disk image icon may appear, with the .dmg file extension. Opening the disk icon reveals an icon to drag into the Applications folder on your hard drive.

How to set space parameter for System Restore

Start>My Computer; (RC); select Properties

On Properties Window select System Restore Tab

Set disk space allocation to about 1000 MB

How to set space parameter for Outlook Express

For temporary Internet files (Outlook Express) and remove same—

Open IE6 select tools on top menu, then Internet Options

Internet options window: Temp Internet Files section

Select delete files button; in next window, click OK

Internet options window: Temp Internet Files section
Select settings button; in settings window set amount of disk space to 1 to 10 MB and click OK

How to remove unneeded programs

Start>Control Panel
In Control Panel select Add/Remove Programs
In next window select each unneeded program and select Remove button and follow Wizard instructions

How to declutter memory

Remove programs by running MSConfig
Start>Run; type in or select entry MSConfig
Next window select startup tab and then select Applications
Then uncheck items to delete
Most are not necessary to run at startup
Remove unnecessary entries
Don't remove antivirus, spyware, pop-up blockers, etc.

How to update Windows

How to update with Windows Update:
Start button>Windows Update

Will scan computer and compare to Microsoft site entries
Present a list of critical or non critical updates
Select all critical updates and choose applicable non critical updates
Restart your computer if indicated

How to run CHKDSK, Disk Cleanup and Defrag

Start>Run: type in CHKDSK and click OK

How to save device drivers

Open Windows Explorer:
Start>All Programs>Accessories>Windows Explorer (double-click to open)
Find Folder C:\Drivers and copy to the backup device
Find Folder C:\Windows\System32\Drivers and copy to the backup device

6 Glossary

adware: a software application in which advertisements are displayed while the program is running. These applications include additional code that displays the ads in pop-up windows or through a bar that appears on a computer screen. Further, see *Malware*.

antivirus software: a program that detects and removes viruses and worms trying to get into your computer via e-mail or other network connections. The simplest kind scans executable files, using a list of known virus definitions. Antivirus software should always include a regular subscription (update service), allowing it to keep up with the latest viruses as they are detected. It does not block intruders from gaining control of your computer. Compare *Firewall*.

backdoor: (trap door) a hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. The function will generally provide unusually high, or even full, access to the system either without an account or from a normally restricted account. It is activated in some innocent-appearing manner; for example, a key sequence at a terminal. Invocation of the backdoor can also be done by sending a specific packet to a network port.

cache: pronounced “cash.” **(1)** a small, very fast (but not addressable by the programmer) memory that serves as a temporary storage area for frequently (or recently) accessed data. Having certain data stored in cache speeds up the operation of the computer for those tasks performed most often.

Mac OS X stores a lot of commonly accessed data (like Finder icons and Extensions data) in its caches to optimize performance. But sometimes the data in these caches does not get updated properly. Here’s the fix:

1. Delete everything in Library>Caches
2. Delete everything in Users>[my account]>Library>Caches
3. Reboot. Do this once a month, and before any OS update

(2) a set of memory and file caches kept by a Web browser or other online program to avoid having to download the same material repeatedly. For example, Microsoft Internet Explorer has a folder on a PC’s hard disk in which the program stores Web pages and other files, such as images, as they are viewed. By storing these files on the hard disk, Internet Explorer can display previously visited pages more quickly, because it displays the files from the hard disk rather than from the Web.

To clear this cache, for example, in Internet Explorer: Tools>Internet Options to open Internet Properties>General Tab>Delete Files>OK; Click OK to exit.

In Safari: Safari Menu>Empty Cache>OR Safari Menu>Reset> Safari>Reset (resetting Safari clears the history, empties the cache, clears the Downloads window, and removes all cookies. In other words, it prevents other people from seeing what you have been doing on the Web)

In America Online: Start>Settings>Control Panel; Double-click Internet Options to open Internet Properties; [Click General Tab, on some versions]; Delete Files. Click OK.

In Firefox: Tools>Options>Privacy>Privacy Properties; click Clear (across from the Cache option); click OK to return to browser main page; exit and relaunch the browser.

NOTE: The search engine, Google, takes a snapshot of each page it examines as it crawls the Web and caches these as a back-up in case the original page is unavailable. If you click on the "Cached" link in a Google search result, you will see the Web page as it looked when Google indexed it. Further, see under Web browser/browser caching.

CHKDSK: a DOS command that checks the record-keeping structures of a DOS disk for errors. CHKDSK checks the validity of hard-drive indexes and file structures.

cookie: a mechanism that allows a Web server to store its own information about you on your own computer. Cookies store information such as username and password, preferences on Web surfing habits, and what parts of the site were visited. The remote server saves the information the cookie contains about the user, and the user's browser does the same, as a text file stored in, for example, Firefox's or Explorer's program folder. The next time you access that site, the information in the cookie is sent back to the site so that information displayed can vary, depending on your past preferences and usage.

Cookies can be programmed to track your steps not only at the current Web site but as you surf from site to site, yielding information to their advertisers and marketers; thus, they are an important privacy factor. Cookies can be viewed by anyone with access to your computer, so it's a good idea to delete all cookies periodically. Not all browsers support cookies.

You do have some control: some browsers can be set up to alert the user when a cookie is being sent so a user can accept it or not. Cookies can be refused, but often you can't proceed further in a particular Web site if you refuse to accept cookies—and there are scads of them in any one Web visit. Compare *Spyware*.

cramming: placing charges for unordered and unwanted services on the customer's bill.

defrag: (defragment) to reorganize a disk by putting files into contiguous order. Because the OS (operating system) stores new data in whatever free space is available, a data file becomes spread out across the disk as it is updated. This causes extra read/write head movement during file re-accessing. Periodically, the hard disk on PCs should be defragmented to put scattered pieces of files together again, speeding up access to files and reducing wear and tear on the hard drive. Copying all the files to another disk can defrag a disk. Programs also exist that will defrag a disk in place by carefully rearranging the files without copying to another disk.

Apple says that you do not need to defragment a Mac OS X system because the system defrags files smaller than 20 MB automatically.

device driver: a small software program that links a hardware peripheral, known as a device, to the OS (operating system) and controls its operation. (A device driver always refers to software, while device always refers to hardware.) When you buy an operating system, many device drivers are built into the product. However, if you later buy a new type of device that the operating system didn't anticipate, you'll have to install the new device driver. A device driver essentially converts the more general input/output instructions of the operating system to messages that the device type can understand.

directory: (folder) an invisible file on a disk where the names, sizes and locations of all other files are stored. A directory simulates a file drawer on your disk, although it's actually an index to files that may be scattered all over the disk. A disk can, and usually does, contain more than one directory, and

directories can contain other directories. However, they do not divide the disk itself into sections or limit the size of a file. Programs and data for each application are typically kept in a separate directory (spreadsheets, word processing, etc.), creating the illusion of compartments or drawers. On the Mac, directories are called folders: System folder, Documents folder, Applications folder, Library folder and so on. And folders can contain other folders.

domain: in communications, all resources under control of a single computer system. In a LAN, a domain is a sub-network comprised of a group of clients and servers under the control of one security database.

download: To download is to receive. In a communications session, to download means to transmit a file or program from a central computer to a smaller computer or to a computer at a remote site.

encryption: the act of scrambling or converting information into a code or cipher so that unauthorized people will be unable to gain access to its content. A secret key or password is required to decrypt (decode) the information. As more and more confidential data is being sent along computer networks, it is increasingly important to develop ways to send information securely.

favorites: (bookmarks) a feature of a Web browser that enables you to record frequently used URLs on a special menu so as to go directly to them in future without having to retype the Web addresses. For example, Internet Explorer has a Favorites Menu on its toolbar. In some browsers, like Safari and Netscape, the equivalent is called Bookmarks.

firewall: a form of Internet security located at a network gateway server that protects the resources of a private network from unauthorized intruders. (The term also implies the security policy that is used with the firewall.) An enterprise (such as University Commons) with a LAN (local area network) that allows its members access to the wider Internet installs a firewall to prevent outsiders from accessing its own private resources. Compare *Antivirus software*.

personal firewall: sometimes called a desktop firewall, it's a software application used to protect a single Internet-connected computer from intruders. Often compared to antivirus applications, personal firewalls work in the background to protect the integrity of the system from malicious computer code by controlling Internet connections to and from a user's computer, filtering inbound and outbound traffic and alerting the user to attempted intrusions. It is like a wall in that it can prevent unwanted traffic from passing either way. However, it does not detect and remove viruses and worms that may invade your computer.

Note: A firewall keeps outside people from breaking into your node, but if you have Wi-Fi it is as if you are taking your inside network and throwing it into the air surrounding you, so a firewall is irrelevant. You must use encryption such as WEP (wireless equivalent privacy).

hacker: an individual who either for profit or amusement tries to take over resources found on the internet. Complete sets of tools on CD are available commercially from hacker websites. A **white hat hacker** is a specialist working legitimately for a firm of public accountants in order to audit the security of its clients' systems.

key logger: (keystroke logger) A key logger captures the computer user's keystrokes—whatever the user types on the keyboard—including credit card numbers, passwords, bank account numbers and other sensitive information. Writing software applications for key-logging is quite easy, and like any

computer program can be distributed as a trojan or as part of a virus or worm that sends that information to the owner of the parasite.

logical vs. physical: high-level (reasoned) vs. low-level (machine level). Logical implies a broader view than the physical. A message transmitted from Phoenix to Boston logically goes between two cities; however, the physical circuit could be Phoenix to Chicago to Philadelphia to Boston.

malware: a collective term including the many varieties of deliberately **malicious software**, that is, software written for the purpose of causing inconvenience, destruction, or the breaking of security policies or provisions. Malware is generally considered to include programs such as viruses, trojans, worms, probes, spyware, adware, and spam. Others include DDoS (distributed denial of service) clients (zombies) and logic bombs (a computer virus that remains hidden until it is triggered when certain specific conditions are met).

pharming: the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the domain name for a site, and to redirect traffic from that Website to another Website. (DNS servers are the machines responsible for resolving Internet names into their real addresses.)

If the Website receiving the traffic is a fake Website, such as a copy of a bank 's Website, it can be used to “phish” or steal a computer user's passwords, PIN number or account number. Note that this is only possible when the original site is not SSL (secure sockets layer) protected. Further, see *phishing*, below.

phishing: (brand spoofing) sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to a Web site where they are asked to “update” personal information. The Web site, however, is bogus and set up only to steal the user's information.

Phishing is a derivative of fishing, the idea being that bait is thrown out with the hope that, while most will ignore the bait, some will be tempted into biting. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organization's site, by spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

ping: (**packet Internet groper**) an Internet utility used to determine if a particular IP address is on line. To ping a machine basically means that you send out a small amount of information, a test data packet, to another computer connected to the Internet. Then you wait for a response from the other computer to see if it acknowledges the communication with your machine. Pinging a computer can be useful if you suspect that a Website or other file server you are trying to reach is offline. For example, if you are not getting any e-mail, you can ping your mail server to see if it is there. If you get no response, the odds are that it is down.

ping flooding: the practice of maliciously disrupting a computer by pinging it continuously, i.e., flooding it with test data packets to which it must respond.

probe: a device or program used to gather information about a system or its users. It often sends pings (inquiries) to find open ports in unprotected computers, with the intent of sending in trojans, worms or

key loggers in order to take over your computer remotely and turn it into a robot for their use. Further, see *Malware*.

product key: a key that is specific to a particular item or unit, such as a CD, a software program or a service. If two people try to register the same product key then the second registration will fail. This anti-piracy technology is built into many products. Consider what happens when you buy a new piece of software that has strong licensing: you are given a unique key with your product, you launch a registration program, and it generates a unique license key that enables your product to work on your computer (and your computer only).

registry: a central hierarchical database used in Microsoft Windows to store information necessary to configure the system for one or more users, applications and hardware devices. The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used.

You can access the registry through Control Panel in My Computer or by using the Properties menu option on the File menu. Remember, editing the registry is extremely dangerous, so take care when doing so.

router: a protocol-dependent device that connects two or more networks at the network layer. It helps break down a large network into smaller sub-networks. It lets you share your broadband connection with multiple Macs or PCs. Many routers act as firewalls to keep out hackers.

scan: to examine, in sequence, with a device that acts upon the information received. Dictionary-based antivirus software characteristically examines files when the computer's operating system creates, opens, closes or e-mails them. In this way it can detect a known virus immediately upon receipt. Antivirus software can typically be scheduled to examine (scan) all files on your hard disk on a regular basis.

security patches: software updates. Updates (a.k.a. "patches," "service packs," "fixes" and "security packages") improve your odds of protecting your computer and your personal data. Updates address exploitable flaws or introduce additional security features. For instance, the Microsoft Outlook E-mail Security Update helps Outlook users protect themselves from certain viruses, as well as diminish the spread of viruses through Outlook.

slamming: the illegal practice of changing a consumer's telephone service—either local or long distance—without the customer's permission.

spam: (UCE, unsolicited commercial e-mail) junk e-mail, nuisance advertising. It's a disruptive message posted on a computer network. Currently most e-mail traffic is spam—and rising rapidly (7 % in '01, 12 % in '02, 48% in '03, 77% in '04; 83% as of 3/05, est. 95% in 06), according to Spamhaus. Two out of three spam e-mail messages contain false information of some sort, according to an analysis of unsolicited e-mail pitches collected by the FTC.

spyware: a program that tracks a computer user's online habits and Web activities and returns the research to the designated source. Spyware is embedded in many free downloads, and some companies quietly include spyware as part of the software they sell. Many people do not realize they

are being watched and followed around the Internet by these stealth programs, which are designed to report back to anyone from marketers to criminals planning identity theft. Examples are Gator, BonziBuddy, Weatherbug and the malicious CoolWebSearch. Other programs capture and store keystrokes and screen views, such as SubSeven and Spector. Programs that can detect and remove existing spies from Windows systems include Spybot Search & Destroy, Lavasoft Ad-Aware Plus and PestPatrol. Spybot will also immunize. Compare *Cookie*. Further, see *Malware*.

SSL: <secure sockets layer> a protocol used by the HTTPS access method. SSL facilitates secure communication over the Internet and is the Internet's leading security protocol. SSL protects the privacy of data exchanged by the Website and the individual user by encrypting the communications and data between the two computers. Most e-commerce Websites use it. When you submit your credit card number or check your bank balance on a Web page that has been specified as secure, the server sends a copy of its SSL certificate to your browser. This certificate is a digital identification card that verifies the site as authentic and allows it to use the SSL encryption for transmitting sensitive data. If you see a small padlock icon in the bottom corner of your browsers or if you are visiting a site with a URL that begins with **https** instead of **http**, you are at a secure site.

surge protector: (surge suppressor) an electrical device that monitors the level of electrical current between a power source and a computer or another electronic component. When the surge protector detects a surge of voltage beyond a certain limit, the circuit is shut down or the level is automatically reduced to prevent damage to the electronics. Voltage surges are created by things like lightning strikes, power-grid surges or by electric motors switching off. Surge protectors do little good unless the power line is properly grounded. Always plug the computer into a properly grounded outlet. If possible, do not plug a laser printer into the same outlet strip as the computer because laser printers draw heavy current intermittently. Many surge protectors also incorporate RFI (radio frequency interference) protectors to help reduce radio and TV interference emitted by the computer into the power line.

System Restore points: A restore point represents the computer's configuration at a given moment in time. Creating a restore point allows you to reset the computer back to this same configuration at some time in the future. Microsoft recommends that you set a System Restore point before installing any digital media components. This enables you to return to your original system configuration, if necessary. Use the following steps to create a restore point:

1. Click Start, Programs or All Programs, Accessories, System Tools, and then System Restore. The Welcome to System Restore window appears.
2. Select Create a Restore Point, and click Next.
3. In the Restore point description field, type anything you want that helps describes the computer's current configuration change. What you type here will help identify the restore point later. For example, "installed racing game," or "added new video card."
4. Click Create. A new screen opens stating that a new restore point has been successfully created. The name of the restore point, the time, and the date appear in red.
5. Click Close to exit or click Home to return to the main System Restore window.

temporary file: a file that is temporarily created by a running application to store information in order to free memory for other purposes, or to act as a safety net to prevent data loss. For example, Word determines automatically where and when it needs to create temporary files. The temporary files only exist during the current session of Word. When Word is shut down in a normal fashion, all temporary

files are first closed and then deleted. However, sometimes when an application closes, temporary files remain and have to be removed manually. They often have a .tmp extension.

trojan: (Trojan horse) a computer program that is either hidden inside another program or that masquerades as something it is not in order to trick potential users into running it, for example, a program that appears to be a game or image file but in reality performs some other function. It pretends to have a beneficial set of features but either instead, or in addition, contains a damaging payload. Compare *Virus*. Further see *Malware*.

TWEAK UI: Tweak UI is basically a safe way to alter registry settings for tweaking different aspects of XP by providing access to system settings that are not exposed in the Windows XP default user interface. Customization of Explorer, Taskbar, My Computer and many other settings are supported by Tweak UI.

typosquatting: (URL hijacking) taking advantage of common typos users make when entering a Web address (URL) into their browsers. Typosquatting relies on the chance that a person who enters a Website address into a Web browser will accidentally enter an incorrect Website address and be led to an alternative address that the cybersquatter owns, for example, [www.microsoft](http://www.microsoft.com).

UPS: (uninterrupted power supply) backup power used when the electrical power fails or drops to an unacceptable voltage level. Small UPS systems provide battery power for a few minutes—enough to power down the computer in an orderly manner. An online UPS provides a constant source of power from the battery, while the batteries are being recharged from AC power. An offline UPS, also known as a standby power system (SPS), switches to battery within few milliseconds after detecting a power failure.

URL: (uniform resource locator) also called Web address, it's a protocol for specifying addresses on the Internet, defining the route to an accessible resource on the World Wide Web or any other Internet facility. It tells the browser where to find an Internet resource. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages.

All Web sites have URLs. A URL is what a telephone number is to a telephone or what a street address is to a house. Because Web site URLs are sometimes long and hard to read, Web browsers have a Bookmark or Favorites feature that gives you the opportunity to save the location (the URL) of sites you'd like to return to.

username: (screen name, account name, unique name) the first part of an e-mail address before the @, it's a unique name you choose to identify yourself via your ISP (Internet service provider) as a registered user, in addition to your password. You then can connect to that ISP via an e-mail client as such. Examples of username: worry76wort, EguQm15.

virus: a self-replicating program that infects a computer by attaching itself to another program or file, and propagating itself when that program is executed. A computer can become infected by files downloaded over the Internet, a local network, by the installation of new software that is infected or via disks inserted into your computer. **Don't** open downloaded .exe, .pif, .src or .vbs files, or e-mail attachments from unknown correspondents. To prevent infection by computer viruses, you should not use any externally provided software before it is checked by a virus-scanning (antivirus) program.

macro-virus: a virus that exploits applications that allow their associated documents to contain executable code, known as a macro. For example, a spreadsheet program may enable the user to embed “macro” commands in a document to automate certain operations; this makes it possible to use that same facility to program a virus into the spreadsheet that can attack users of that program.

The most pandemic viruses in the mid-to-late 1990s were macro-viruses for Microsoft Office software such as Word and Excel. Later in the 1990s, Microsoft's Outlook e-mail program (which has scripting features) became the most popular vector, as it is today. It enables viruses to spread by e-mailing themselves to the contacts stored in the user's address book.

A particularly dangerous feature of macro-viruses is that they are sometimes able to infect computers running different operating systems and platforms. For example, a macro-virus in a Microsoft Word document can infect users of Microsoft Word on Apple Macintosh computers as well as Microsoft Windows.

virus definition: a known virus pattern. Antivirus software uses a list of known virus patterns to scan your computer. Your virus software needs to be updated regularly in order to protect your system(s) from the new viruses being discovered every day.

Web browser: a computer program that allows you to read hypertext documents on the World Wide Web and navigate between them. A Web browser gives you access to the Internet and helps you retrieve encoded documents in a form suitable for display on your computer screen. In order to view a site, you type its URL (its Web address) into the browser's location field, and the home page of that site is downloaded to you. Browsers have a bookmark feature that lets you store references to your favorite sites. Instead of typing in the URL again to visit the site the next time, you select one of the Bookmarks (Favorites). Popular Web browsers include Microsoft's Internet Explorer, Mozilla's Firefox and Apple's Safari.

Wi-Fi: (802.11b, called Airport on a Mac) a wireless data networking protocol generally used to connect personal computers and laptops to a network. It is the most common means of wireless networking. It allows computers equipped with special network cards to connect wirelessly over a radio frequency to a ground station (Wi-Fi antenna).

WEP: (wireless equivalent privacy) a security protocol for wireless networks, it is designed to provide security equivalent to that available in wireless networks Unlike an Ethernet network, which connects its users through cables, a wireless network sends data through the air on radio waves, making the information vulnerable to anyone with a wireless network card. The primary purpose of WEP is to prevent eavesdropping, but it has the important secondary benefit of preventing unauthorized use of one's wireless network.

Technology Committee members:

Michael Nolte
Al Feuerwerker
Brad Bates

Diane Kirkpatrick, esp. Macintosh

Tony Morris

Keith Scott

Bill Stebbins

Ruth Lehman, Macintosh