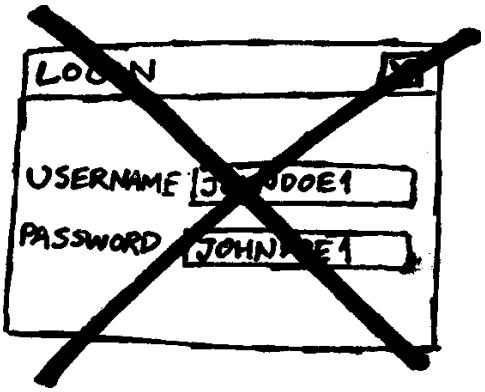
COMPUTER SECURITY FOR THE AVERAGE ACTIVIST

Computer security isn't a complicated concept... its really just a matter of simple procedures you can follow to guard your personal data. Use the following tips to keep your files safe!

Keep your passwords secure!



> **NEVER** give your passwords out to anyone, unless you are giving it to an authentic tech support person or network administrator, and ONLY if they have a legitimate reason--always be skeptical when people ask for your password.

>**DON'T** use simple passwords. Avoid easy to guess passwords like the names of friends, family, pets, or birthdays. Also avoid using common words for passwords. The best passwords combine numbers, letters, and assorted other characters (like the following: @!$%*&, etc.) when possible. The best passwords are random combinations of these things and are at the very least 8 characters long.

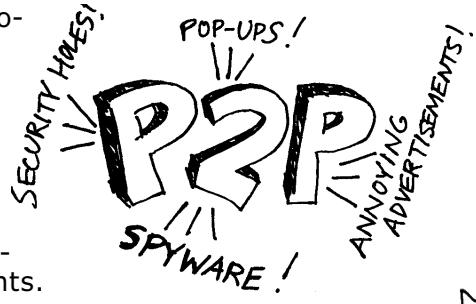
>**NEVER** make your password the same as the login name. Potential intruders often try the same login and password first, as so many people make this fatal mistake.

>If you ever have to write down passwords and login names in the event you have trouble remembering them, keep this information hidden in a secure place AWAY from the computer.

USE ANTI-VIRUS SOFTWARE!

DoIT offers **free** Norton Anti-Virus to students... download it at www.wisc.edu/wiscworld/nav.htm

PEER-TO-PEER: A Security Risk??



Many popular peer-to-peer file trading programs such as Kazaa and Morpheus include secretly installed software called "spyware" which can transmit personal info and bombard you with annoying advertisements. Sometimes Peer-to-Peer programs also leave your system open to snooping, so beware of using P2P software if you're truly paranoid about people potentially accessing your data. If you still want to use P2P but keep your data secure, either use your program's features to block other users from accessing your files or carefully limit which folders on your system are shared. To remove spyware/adware from your system, try AdAware, a free spyware scanner: www.lavasoft.de

Beware of your e-mail! Look before you open...

> **AVOID** opening files that come attached to your e-mail, unless you absolutely know what that file contains, who it is from, and if it can be shown to not contain any virus or "trojan horse" programs. Use a **virus scanner** when possible to scan any attachments before opening them.

> **BEWARE** of suspicious looking messages. If you receive a message from someone you don't recognize, avoid opening it, especially if it has a questionable subject line. Many new "worms" (a type of computer virus) can unleash themselves on your system just by reading an e-mail... you don't even have to open an attachment. The risks of this can be avoided by turning off any scripting features in your e-mail program... and often these worms specifically target e-mail programs from a certain company whose name starts with "M" and ends with "icrosoft," so you just might want to consider avoiding that particular e-mail software.

Got secrets? Encrypt them!

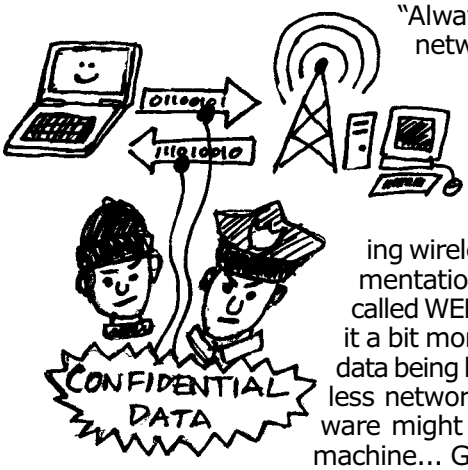
If you have to e-mail things you want to keep secure, or want to prevent snoops from looking at certain files, consider using encryption software. Encryption software takes the contents of a file and scrambles it all up into an unintelligible pile of what appears to be nonsensical data--that is nonsensical only if you don't have the decryption key! Some of the best encryption software currently available is PGP ("Pretty Good Privacy") or GnuPG (the GNU Privacy Guard). You can find this software at the following websites:

PGP- www.pgpi.org

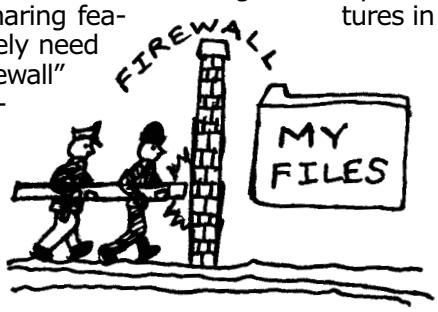
GnuPG - www.gnupg.org

Remember, as a general rule when using encryption, the longer the encryption key, the stronger the encryption (i.e. 512-bit is better than 64-bit)

"Always On" and Wireless Connections, a wide open door...

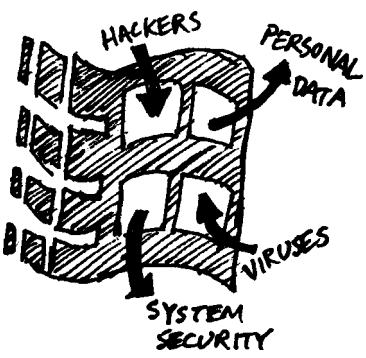


"Always On" internet connections (such as cable, DSL, or ethernet) and wireless networking solutions are a convenient way to connect your system to the wonders of the internet, but they also make your system a prime target for hacking. That is unless you take the proper precautions... when using an "always on" connection, turn off any file and printer sharing features in your operating system (unless you absolutely need them turned on), and consider installing a "firewall" program that helps block intruders. When using wireless networking systems, consult your documentation to find out how to turn on a useful feature called WEP (Wireless Encryption Protocol)--it will make it a bit more of a challenge for people to snoop on the data being beamed around your wireless network. Wireless networks are another area in which firewall software might be a good thing to have running on your machine... Generally firewall software is not entirely free, though you can get some stripped down versions of firewall software such as Zone Alarm. Here are some addresses to find firewall software: Zone Alarm: www.zonelabs.com TinyFirewall: www.tinysoftware.com BlackIce: www.networkice.com McAffee and Symantec (a.k.a. "Norton") also offer firewalls along with some of their antivirus software packages.



Patch Security Holes

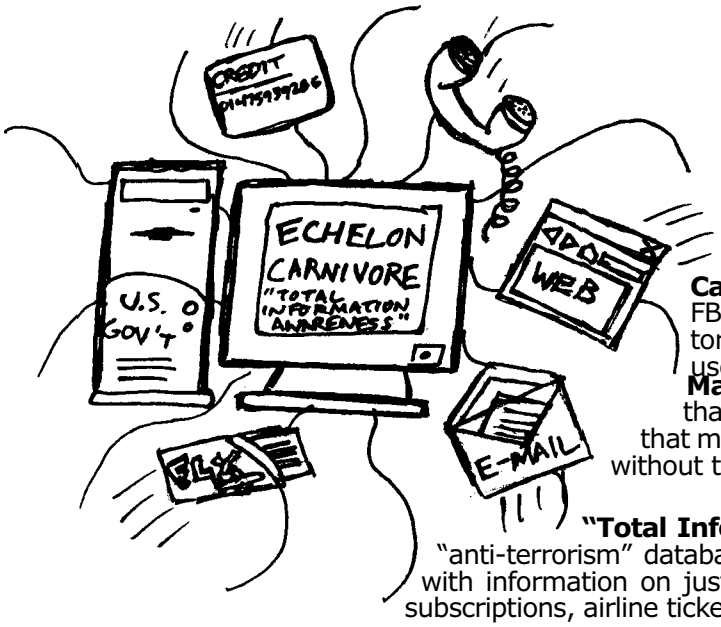
Many programs have various security holes in them which leave your system wide open to hackers and other people with malicious intentions... always make sure your software has up to date "patches" to close any known security holes. Also, if you're really paranoid about security, try to avoid using software with a known track record of security flaws. Not to single out Microsoft, but Windows, Internet Explorer and Office have all had a history of major bugs... a possible alternative to some of these programs is in open source software like Linux and OpenOffice. You can check out an archive of open-source software for Windows at the following address: http://gnuwin.epfl.ch/



Other Tips for Computer Security

> **Just because you press Delete doesn't mean its gone!** If you need to get rid of some files, just dragging them to the trash or pressing the delete key won't do the trick. Remember to *empty* the Recycle Bin/Trash on your system to actually delete the files. Also, even when a file appears completely deleted to a user, it is often still floating around on a disk and can be recovered if you have the right tools around... to make sure something is *really* gone, use a secure deletion program. PGP encryption software includes one, and others are easy to find on the net.

> **"Anonymous" is not always Anonymous** No matter how anonymous you try to be on the net, you leave little clues as to your identity all over the place. For instance, Hotmail and other free e-mail services usually transmit the IP address of your computer along with each message sent. If you want to be totally anonymous on the internet, try an "anonymizing proxy" service like Anonymizer (www.anonymizer.com). These route your internet traffic through a third-party computer which masks your identity. Often there is a charge to use these services, but if you're that paranoid, it might be worth the money.



A Glossary of Threats

Echelon: A secret computer system managed by the US National Security Agency along with UK, New Zealand, and Australian authorities. Supposedly a massive surveillance archiving system for international electronic communications such as e-mail and telephone.

Carnivore: The e-mail and web equivalent of a wiretap, this FBI software is placed on an internet provider's servers to monitor the internet communications of a specific user or group of users.

Magic Lantern: Codename for secret FBI keylogging software that is deployed on an individual's computer to log all activity on that machine. Rumored to be installed secretly through e-mail, even without the user actually opening the message.

"Total Information Awareness": Concept for new Dept. of Defense "anti-terrorism" database that creates a super database from different databases with information on just about everything you do... credit card records, magazine subscriptions, airline tickets, phone calls... It's the closest thing to "Big Brother" yet...