

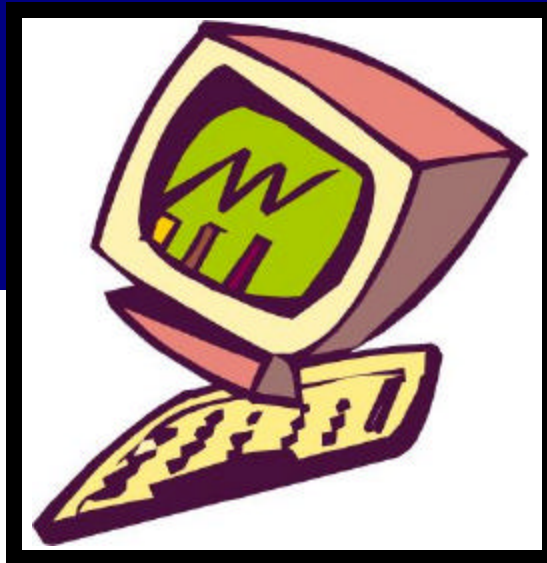
Computer Security

Suggestions for our users:

There are several measures computer users can take to ensure they are not exposed to unnecessary risks. For some, being secure on the Internet will require a profound modification of computer habits. Following are some important recommendations to assist you. Our Network Team has also taken many security measures to protect our users. Please do not hesitate to contact WJH Computer Services if you should have any questions or concerns.

Here are five suggestions on how to make the Internet experience safer for you:

1. **Data Files:** "If you work without a net, you're more likely to fall." In theory nothing can ever be 100 percent secure. There is always a chance that your computer will be hacked, stolen or otherwise destroyed. Prepare for this! Store all sensitive information on some form of storage media that is not attached to the computer. Try to adopt the philosophy that if someone did gain access to your machine, they would not obtain valuable data.
2. **Antivirus Software:** Use antivirus software. Antivirus software is the single most important piece of software on home or work computers. There are a number of excellent products on the market. Web sites such as www.freeware.com, distribute free and trial version of numerous antivirus software packages. McAfee/Virex is the Harvard supported package.
3. **Electronic Mail:** E-Mail is a severe security problem. Never open unsolicited e-mail attachments. People never learn that the cute little *Pokemon* animation that your best friend sends you may actually be the next "I love you" virus. Don't open it! Make it a habit of only opening e-mail attachments that you explicitly requested. Malicious e-mail attachments are not the only e-mail related danger. Users should treat e-mail communications as though they were shouting in a crowded room. Unless e-mail messages are encrypted, anyone can read them. Confidential communications should always be encrypted. After being sent from your computer, e-mail travels all over the Internet and can be read by anyone whose path it crosses.



4. **Personal Information:** Personal information must be protected. It's amazing how much information can be learned about a person from their phone number. The users' key asset is their personal information, and this should be zealously guarded. When surfing the web, installing a program, or

chatting in a chat room, always be skeptical. By creating online profiles and storing your personal information on your computer, you eliminate one of the original security features of the Internet, anonymity. Companies such as ZeroKnowledge make privacy solutions that can help preserve your personal information, and protect you from web pages and applications that attempt to remove your personal information from your computer without your consent.

5. **Passwords:** Choose strong passwords. Passwords are a broken security scheme. They are clumsy, relatively easy to crack, and the better a password the harder it is to remember. Passwords should be at least eight characters long and contain letters, numbers, and special characters. When creating a password never base it on a word found in the dictionary. Try to make it as random as possible. One approach that works well is to think of a sentence that you will never forget. For example, "Don't forget to take out the garbage on Friday" is fairly easy to remember and has some practical connection to everyday life. Now convert the sentence into a password. Take the first letters of each word "Dfttotgof" and come up with a scheme for further jumbling them. You can replace the f with a 5, since they look similar, and the o's with 0's. Next replace the letter g with a special character like "&". You now have "D5tt0t&05", a very difficult password to crack. Now that a strong password has been created, don't write it down on a sticky note that gets stuck on your computer. If you must write down your password store it in a place to which only you'll have access.

Send comments or questions to help@wjh.harvard.edu or call 617-495-3811.

William James Hall Computer Services