



Safe Computing at CUMC

eSupport immediate help online: <http://support.cubhis.org>
5-Help (212-305-4357) 5help@columbia.edu www.cubhis.org

This document contains basic information that will help you keep your computer and data safe both on and offline. When you open an email account or connect a computer to the CUMC network, you gain many privileges - which come with considerable responsibility. Being informed and responsible when using the network prevents your computer and your Columbia (UNI) account from falling prey to malicious behavior. In addition, you must be aware of certain legal issues related to network activity, or you risk running into legal and/or academic trouble.

Computer Security is Your Responsibility – The security of the Columbia network depends on the security of each computer connected to it. You are ultimately responsible for all of the network traffic that passes through your system and must maintain the security of any computer you connect to the campus network. If you fail to do this, your system could become infected with a malicious program that might destroy a term paper or dissertation, or possibly steal your credit card number. The University Email System protects you from most known email viruses and works to reduce spam in Columbia accounts, but you must still protect your computer and account by practicing safe computing.

Computer and Network Use Policy

The Columbia University Computer and Network Use Policy, which governs all online activities at Columbia University, can be found at <http://www.columbia.edu/cu/policy>. Policies specific to the CUMC campus can be found at http://www.cubhis.org/getting_started/policy.html - because this campus shares its network with New York Presbyterian Hospital and must comply with Health Insurance Portability and Accountability Act (HIPAA) regulations, there are additional security procedures that must be followed:

- All systems must be registered with current contact information prior to getting network access
- No gaming or networking devices (routers, wireless access points, etc.) can be set up on the network unless approved by a school's Dean or done in conjunction with CORE Resources
- All systems should run current antivirus and antispyware programs
- All systems should run operating system updates to ensure that any critical flaws are patched

For additional information regarding registering for network access please contact CUMC IT's Service Desk, the Information Commons, directly. Please also see the reverse side of this document for further instructions on computer and account security.

Be aware of copyright and intellectual property laws. If you purchased an item such as a pre-recorded CD or DVD you may keep an electronic copy on your computer. If you do not have a purchased copy, you may not have a copy on your computer – that is copyright infringement, a federal crime. Even if you own a copy of an item, it is illegal to download or share it.

Do not enable file sharing on your computer if it allows access to others' copyrighted works. Columbia University has received hundreds of complaints of copyright infringement from the music, software and motion picture publishing associations as a result of people sharing or possessing copyrighted material on their computers. You could lose access to the Columbia University network and possibly to your email account if you violate copyright laws. In addition, you can be sued by the copyright holder for damages if you are found possessing and/or sharing copyrighted material that is not legally yours. Please see <http://www.columbia.edu/cu/policy/copyright-info.html> for more information.

Unacceptable behavior in a non-cyber setting is also unacceptable in a cyber setting. The consequences of harassing, stalking, or threatening someone online result in the same legal consequences as they do offline. Attempts to compromise systems and networks are also considered serious offenses, and can result in suspension from the University and even criminal prosecution.

System Security

Here are some important steps you can take when using your computer to protect the system itself, your data, and your personal information:

Avoid opening web site links from an email or instant message. Be wary of email and instant messages containing URLs that you weren't expecting. Opening a web page from an email message can be just as dangerous as opening an attachment. The past years have seen a significant rise in "Phishing", where a web site or email seems authentic but is actually an attempt to steal personal identity information.

Use Symantec Endpoint. You can download Symantec for free as a Columbia student, faculty or staff member by going to <http://www.columbia.edu/acis/software/nav>. Keep your virus definitions up to date by enabling the included LiveUpdate program. Set this program to update your virus and spyware definitions automatically and daily, as new malicious programs are discovered very frequently.

Use Windows Defender. Microsoft's antispyware program has received great reviews and is available for free: <http://www.microsoft.com/defender>

This application protects your computer from spyware, trojans, keystroke loggers and other malicious programs as well as unwanted cookies. **NOTE:** If you are using the latest version of Symantec (Endpoint/version 11), a built in antispyware program is included.

Keep your operating system patched and up to date. New vulnerabilities in operating systems are regularly discovered and exploited. To prevent virus infection or worse due to this, use a built-in update program and set it to update automatically: Windows Update for Windows and Software Update for Mac OS X are two examples. You can learn how to use these programs at <http://security.columbia.edu>. If you use an operating system other than Windows or Mac, get on a mailing list such as CERT Alerts (<http://www.cert.org>) to receive information about updates for your computer's OS.

Protect your laptop. Never leave your laptop unattended. They are easily stolen even when locked, and cable locks can be cut off and easily removed. In addition, Columbia provides the laptop security program PhoneHome for students, faculty and staff at no cost via <http://www.columbia.edu/acis/software/pcphonehome/>. The program will attempt to locate your laptop if stolen, however please be sure to read the FAQs linked on this site before installing for full information on how it operates.

Account Security

Your email ID (UNI) and password are the keys to a great amount of personal information about you, such as your grades, homework submissions, home address and Social Security Number. Here are some important yet simple ways to protect yourself and your account information:

Keep your password secret. Never give your password to anyone, not even a spouse or best friend. In fact, it is against Columbia University policy to share your password with anyone! Also, be sure to use strong passwords that contain both letters and numbers on all of the systems that you log in to, and don't use the same password everywhere.

Do not save your email password on your computer. Enter it every time you open your email program, even if you think no one else has access to your computer.

Log out of public terminals completely! Otherwise, you may have just given the next person unlimited access to your accounts.

Never send confidential information via email even when the messages are encrypted. There's no telling what a recipient will do with that information, whether by accident or with malicious intent.

Use a screensaver password. This is strongly recommended. Do not use your email password for your screensaver. In Windows XP and Vista, go to *Start - Control Panel - User Accounts* (Vista users may have to select **User Accounts and Family Safety** first), select the account you're using and the *Create a password* link. On Mac OS X, open *System Preferences* from the Apple menu and select *Accounts*, then *Change Password*.

For more information, please see http://www.cubhis.org/getting_started/safety.html or contact the Information Commons service desk at (212) 305-Help and 5help@columbia.edu