



5-Help (212-305-4357), option 5
5help@columbia.edu • <http://www.cumc.columbia.edu/it>

CUMC computer security and policies 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 could destroy a dissertation, send out spam email from your computer, attack and attempt to hack other computers, or even find your passwords, social security and credit card numbers. The University Email System protects you from most known email viruses and reduces 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.cumc.columbia.edu/it/policy>. Because this campus shares its network with New York Presbyterian Hospital and must comply with current Health Insurance Portability and Accountability Act (HIPAA) regulations, there are additional security measures that must be followed:

- All systems must be registered with current contact information prior to getting network access
- All systems must run current antivirus and antispyware programs with their recent updates
- All systems must run operating system updates to ensure that any critical flaws are patched
- Automatic email forwarding to outside companies cannot be configured on CUMC student accounts
- No networking devices (routers, wireless access points, etc.) can be set up on the network unless approved by a school's Dean and done in conjunction with CORE Resources

For additional information regarding network and account access please contact the CUMC IT Service Desk directly. 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 purchased, downloaded electronic copy of an item, it is illegal to 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 immediately 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.

Continued on other side

System Security

Below are a list of measures that must be taken to fully protect your computer, data, and 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 already expecting. Opening a web page from an email message can be just as dangerous as opening an attachment. The past years have seen a huge rise in "Phishing", where a web site, email or instant message seems authentic but is actually an attempt to steal personal identity information.

Use Symantec Endpoint - <http://www.columbia.edu/acis/software/nav>. Symantec is free for students, faculty and staff. 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 constantly being released.

Keep your operating system patched and up to date. New vulnerabilities in operating systems are regularly discovered and exploited. To prevent virus infections or worse, 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 OS 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 mobile devices. Never leave a laptop, tablet or smartphone unattended. They are easily stolen even when locked; cable laptop locks can be cut off and easily removed. Columbia provides the laptop security program Phone-Home at no cost via <http://www.columbia.edu/acis/software/pcphonehome/>. It will attempt to locate your laptop if stolen; be sure to read the FAQs linked on this site before installing for full information on how it operates. Other mobile devices must adhere to policies found at http://www.cumc.columbia.edu/it/getting_started/policies_phone.html

Encrypt the data on your computer, USB keys, and other media. Data on your computer or any other media such as USB keys/flash drives, and compact and DVD discs can be easily encrypted in a way that is transparent to you. This prevents information from being discovered if the computer or media are stolen or lost, and is a vital consideration for anyone affiliated with CUMC whether you regularly work with patient health information (PHI) or not. See <https://secure.cumc.columbia.edu/cumcit/secure/security/encryption.html> for encryption recommendations.

Account Security

Your email ID (UNI) and password are the keys to a great amount of personal information about you and your work. Following are important yet simple ways to protect yourself and the data that can be accessed with your accounts.

Keep your password secret. It is against Columbia University policy to share your password. You must never give it to anyone, not even a spouse or best friend. Also be sure to use strong passwords that contain both letters and numbers on all of the systems that you log in to, and do not use the same password for everything.

Do not set automatic forwarding on your Columbia email account. Medical Center affiliates must adhere to HIPAA and the HITECH act which have specific data and email encryption policies. To avoid release of PHI data, accidental or otherwise, CUMC students cannot automatically forward their institutional email to an external account including Gmail, Yahoo mail, etc. Severe legal and financial fines can be incurred if sensitive data is released, see http://www.cumc.columbia.edu/it/getting_started/email_policies.html for details.

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

Log out of public terminals completely! Otherwise, you may give the next person full 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. But, do not use your email password for your screensaver. To set one in Windows go to *Start - Control Panel - User Accounts* or *User Accounts and Family Safety*, select the account you're using and the *Create a password* link. On Mac OS X, open *System Preferences* and select *Accounts*, then *Change Password*.

For more information, please see <http://www.cumc.columbia.edu/it/safety> or contact the CUMC IT Service Desk at (212) 305-Help, option 5, and 5help@columbia.edu