

KALEIDOSCOPE

Library and Information Services

Supporting a Community of Learners

The Recording Industry Association of America (RIAA) has been waging an aggressive and highly-publicized campaign to identify and sue people who share music files. They have targeted college students who, it believes, are some of the worst offenders.

Please be aware of the impact here on campus. If you choose to use file-sharing software and share media files over Wheaton's network, you may be identified and sued. Wheaton College cannot protect you.

It is your responsibility to protect yourself *and* the health of our shared network. File sharing (peer-to-peer, P2P) applications such as Kazaa, BitTorrent, Gnutella, and eDonkey can leave your computer and Wheaton's network vulnerable, disrupting network performance for everyone. Review this issue of Kaleidoscope and incorporate its advice into your routine computer care.

Members of Wheaton's Library and Information Services (LIS) division monitor the changing legal landscape and RIAA's actions carefully. LIS will publicize changes to related college policy, as appropriate.

So far this year, RIAA subpoenas have identified nearly two thousand individuals, including many who used their college or university networks to distribute copyrighted music. The RIAA uses the "John Doe" litigation process to sue people whose names are unknown. The lawsuits identify the defendants by their numerical computer address, known as an "IP" or Internet Protocol address. Once a "John Doe" suit has been filed, the plaintiffs can subpoena the information necessary to identify the defendant by name. The move follows a decision by a federal appeals court that the information subpoena process allowed by the Digital Millennium Copyright Act (DMCA) cannot be used in infringement cases involving peer-to-peer networks.

Subpoenas have been served to many of Wheaton's "neighbor" colleges and universities including Bentley College; Boston College; Boston University; Brown University; MIT; and Northeastern University. Other educational institutions have included Emory University; Georgia Institute of Technology; Gonzaga University; Mansfield University; Michigan State University; Princeton University; Sacred Heart University; Texas A & M University; Trinity College (Conn.); Trinity University (Tex.); University of Kansas; University of Minnesota; and Virginia Polytechnic Institute.

Source: <<http://www.riaa.com/>>

If you choose to use file-sharing applications and share media files using Wheaton's network, you may be identified and sued.

Wheaton College cannot protect you from current United States copyright laws.

FREE MUSIC! ?



Library of Congress, Prints and Photographs Division [reproduction number, e.g., LC-USZ62-110212]

Let's rock, everybody, let's rock. Everybody in the whole cell block was dancin' to the Jailhouse Rock.

Words and music by Jerry Lieber - Mike Stoller

Official Wheaton College File Sharing Practice

Downloading and storing copyrighted music and movies from the Internet to your personal computer is illegal and a violation of two campus policies: the College Honor Code and the Acceptable Use of Campus Network and Computing Systems Policy <<http://www.wheatoncollege.edu/policies/aup.html>>.

Further, you should take extreme care to ensure that copyrighted material (whether you own it or not) is not being distributed through the use of a peer-to-peer (P2P) file sharing application that you may have installed on your computer.

The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) vigorously pursue infringements of copyrights owned by their individual members, as is their right under U.S. Copyright Law. Every semester many complaints are lodged by these organizations against members of the Wheaton College community. Under the Digital Millennium Copyright Act (DMCA), college administrators are required to cooperate in the pursuit of alleged violators.

Use of P2P file sharing applications is not strictly forbidden on Wheaton's network. That is, installing and using a P2P application by itself does not constitute unacceptable behavior. However, use of these applications can consume an excessive amount of bandwidth and place unnecessary strain on the college's local area network. These actions, especially for non-academic pursuits, can also be a violation of Wheaton's Acceptable Use Policy.

For these reasons, file sharing is limited to a small fraction of the capacity available on our connection to the Internet. File sharing applications are not denied bandwidth altogether; they are however, given lower priority. For example, P2P applications are allocated restricted bandwidth during the college's normal business hours (8:30-4:30, Monday-Friday).

The college does not monitor P2P traffic per se. However, if we are contacted by either the RIAA or

the MPAA or, while researching the consumption of a large amount of bandwidth by a particular computer, we determine that there has been a copyright violation, the following actions will occur:

First offence:

- You will be notified by email and paper mail that we believe a copyright violation has occurred and you have 48 hours to demonstrate that you have permission to distribute the material or to stop distributing the material.
- The Dean of Students Office will be notified of the policy violation and may decide to take the matter to the College Hearing Board.

Second offence:

- In addition to the actions above, your access to the campus network will be removed for the remainder of the semester in which the violation occurs.

Third and subsequent offences:

- The Dean of Students Office will be notified of the policy violation and the matter will be referred to the College Hearing Board, which may impose additional sanctions. Your access to the campus network will be removed until the Hearing Board decides the case. See <http://www.wheatoncollege.edu/it_s/guides/sharing.html>

KALEIDOSCOPE

SUPPORTING A COMMUNITY OF LEARNERS

Kaleidoscope is a non-technical look at the dedicated people, information services, and technologies that support Wheaton's collaborative learning community. Published two to three times a year, *Kaleidoscope* includes contributions from members of the Library and Information Services (LIS) division (formerly Academic Computing, Information Technology and Services, and the Madeleine Clark Wallace Library). Look for service news, and explorations of technology-enhanced learning, and teaching ... on-campus, and beyond.

Your suggestions are welcome.
Marcia Grimes (mgrimes)
Colleen Wheeler (cwheeler)

Wheaton

Protect Yourself from Digital Danger



Wheaton Student Virus Practice

Student-owned computers that are infected with viruses continue to be a serious problem on the Wheaton network. Library and Information Services becomes aware of an infected computer when it begins to attack the college's servers and staff workstations.

If you allow your computer to become infected you put your files, your computer, and the college's infrastructure at risk. While many viruses are more annoying than damaging, some are designed to erase all of the contents of your hard drive or designed to destroy computer memory that effectively prevent the computer from being used.

Any student computer that is found to be infected will be removed from the Wheaton network. During that time the student will be expected to obtain anti-virus software, install it, and use it to clean the computer of all viruses. Technology Support will assist you. They are currently not charging for that service.

If your computer is found to be infected a second time in any given semester, there will be a \$50.00 fee to reconnect your computer to the network after it is cleaned. If there is a third occurrence of a computer infection in a semester, you will not be allowed to reconnect your computer to the network until the beginning of the following semester and you have paid a reconnection fee.

Please note: You will still be able to use all of Wheaton's public access computers in the Library Atrium and KACC while your computer is off of the network.

All student-owned computers on the residential network must have anti-virus software installed and updated regularly. You do not have to use the software provided by Wheaton. If you are running a Microsoft operating system (XP or Windows 2000), you also need to make sure that your Microsoft operating system is current for any vulnerability by updating it from the Microsoft site.

If you have any questions or need assistance with your computer, contact Technology Support at x3900.

You can help protect our critical network and data assets.

Here's how. Review and act on the content of this newsletter. Adhere to the college's Acceptable Use Policy (AUP), use virus software, practice good password management, and protect privacy. As always, please call Technology Support (x3900) if you need help with password changes or have any other computer support questions.

Change Your Passwords

1. For general electronic services, like email and file services, go to the password changing page on the IT&S web site at http://www.wheatoncollege.edu/IT_S/email/. This can be done whether you are on- or off-campus.
2. For WINDOW, after logging into WINDOW, select 'Personal Information' and the PIN change option is available. Note that WINDOW requires a 6-character PIN.
3. For Blackboard, after logging into Blackboard, select 'Personal Information' and then the password change option.
4. For Banner, after logging into Banner, type GUAPSWD into the Direct Access space.
5. For Meeting Maker, after logging into Meeting Maker, select 'Edit' and then 'Preferences' and it will take you to the password change form.

Clear the Cache on the Public Computers You Use

Do not walk away from a public or shared computer unless you have first logged out of every single service you've touched during that session. Just closing a window is not enough. Look for a "log out" button – use it – and then quit the application.

Most web browser software applications save some information about your activity and reuse it as you work to improve their performance. Although convenient during your session, this practice can make your personal information vulnerable. Safeguard yourself and your personal information by clearing this information out of the browser's memory before you walk away from a public machine... every time.

Here's how to clear a browser's cache file:

Internet Explorer (Windows):

Tools > Internet Options > Temporary Internet Files > choose Delete Files

Internet Explorer (Macintosh):

Edit > Preferences (see screen snapshot)

Safari (Macintosh):

Safari > Empty Cache

The upcoming version of Macintosh's OS X.3, Panther, automatically protects your Home directory using 128-bit encryption.

Keep Your Private Information Private

Information you value is being kept online; if you are not careful other people can steal it. When you think of all the places that private information may live online, you'll want to get into good habits now.

Most people pay no attention to this kind of warning until it's too late. If you're not careful, others can review and steal your:

- personal identity,
- financial information (online banking, payroll data),
- personal email message (in fact, leaving your account "open" allows others to send unauthorized email from you), and
- data files (networked file space like dropboxes).

Your privacy will be compromised if you are sloppy about it. Remind your friends about this, too, since anyone's carelessness can make our entire network vulnerable to hackers who are looking constantly for weaknesses to exploit.

Do:

- Review and act on the "Good Password Management" section.
- Use the computer virus protection the College makes available to you **at no cost**.

Do not:

- Let your browser "auto-complete" web forms.
- Leave your room or office unlocked when you're not there.
- Send sensitive print jobs to an unknown printer.
- Prop open doors to campus buildings.

Spyware and Pop-Ups

The information below contains a brief description and some helpful steps you can take to rid your computer of spyware and pop-ups. It may be helpful to print this information to follow it. http://www.wheatonma.edu/IT_S/support/SpywareEtc.html

Spyware

Spyware, malware, scumware, adware, etc., whatever the term, we're talking about programs that secretly gather information, hijack browser homepages, pop-up ads, or a host of other unwanted activities. These programs are often installed without your knowledge or permission. In addition to the behavior above these programs will slow your computer, increase network traffic, and can be a conduit for virus infections.

Spyware can be installed in a number of ways – via unscrupulous websites, by viruses, or by other programs (most notably P2P File Sharing apps like Kazaa). The best defense against these programs is prudence. Don't install an application from a vendor (shareware, freeware, etc.) unless you know you can trust them. Read the End User License Agreements (EULA) of all the programs you install to make sure you're not agreeing to install Spyware. Periodically check your Add/Remove programs control panel to be sure everything installed should be there.

Install an anti-spyware application such as SpyBot, keep it updated, and scan regularly. Many of these programs, like SpyBot, have immunization functions to actively prevent infection by these programs. SpyBot can be found on the college Software server. The Spyware threat is second only to viruses. Bear in mind that most computer companies, like Dell for example, don't warranty their equipment against viruses or Spyware and won't help in their removal.

To see if you have spyware installed on your computer and to remove it:

1. Download SPYBOT from our software server and install it. (Directions to the software server can be found at the end of this page).
2. Once SpyBot is installed it must be updated with the latest definitions. Do this by clicking on the Check for Updates button (located under the Online Tab in Advanced Mode). If updates are detected download them.
3. Once the updates are installed click on Check for Problems to scan the computer. The scan will take several minutes after which it will list all of the problems it found.
4. Click the Fix Problems button to remove the spyware programs.

Further information on Spyware and its removal can be found on the following sites:

<http://www.cexx.org/adware.htm>

<http://www.spywareguide.com>

<http://www.pchell.com/support/spyware.shtml>

Pop-Ups

We've all seen them! They are those annoying ads that pop-up and in some cases continually pop-up while we are surfing the Internet. Pop-ups are scripted to attach themselves to some websites and to pop-up when you visit them. Usually, they are advertisements for products and some can be very misleading. They can appear on your screen as a warning message telling you that your computer is about to crash or that someone is stealing your data. They can even pop-up to tell you that you have just won some money, NOT!

To stop pop-ups:

Try downloading the Google toolbar at <http://toolbar.google.com/>.

(Please note that using this type of software may interfere with some applications you may be running such as Webfocus or email. You may need to turn this feature "off" and in some cases uninstall it.)

To stop pop-ups while using AOL's Instant Messenger:

<http://www.kb.cert.org/vuls/id/907819>

Your use of the college network indicates your acceptance of Wheaton's "Acceptable Use of Campus Network and Computing Systems" Policy.

Review it by visiting the IT&S homepage and clicking on the "Security" button.

http://www.wheatoncollege.edu/IT_S/

Learn more at http://www.wheatoncollege.edu/it_s/.