



KALEIDOSCOPE

Academic Computing • Information Technology and Services • Madeleine Clark Wallace Library

Supporting a Community of Learners

What's The Big Deal About Sharing Music?

During your summer vacation, the Recording Industry Association of America (RIAA) stepped up its campaign to identify and sue people who share music files. RIAA is particularly interested in targeting college students, who, it believes, are some of the worst offenders. Since late June, the RIAA has issued about 300 identity-seeking subpoenas each week. The subpoenas have been served to ISPs and universities, including Wheaton "neighbors", Boston College, MIT, Northeastern and Boston University.

It's a pressure-packed situation and there are strong opinions on every side of the issue. RIAA's aggressive action has been lauded by some and reviled by many more.

We want you to know how things stand right now, as you return to Wheaton for a new year. It's very simple: if you choose to use file-sharing software and share media files using Wheaton's network, you may be identified and sued. Wheaton College cannot protect you.

It is your responsibility to protect both yourself and the health of our shared network. File sharing (peer-to-peer, P2P) applications such as Kazaa, Grokster, Morpheus and Napster can leave your computer and Wheaton's network vulnerable, affecting network performance for everyone.

IT&S will watch this situation very carefully and publicize changes to related college policy, as appropriate.

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

We want you to know how things stand as you return to Wheaton.

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

Wheaton College cannot protect you.

Official Wheaton College File Sharing Practice

You should take extreme care to ensure that copyrighted material 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 the Wheaton 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 local area network. These actions, especially for non-academic pursuits, can be a violation of the **Acceptable Use Policy*** and may result in sanctions imposed by the Dean of Students Office and/or the College Hearing Board.

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 normal business hours of the college (8:30-4:30, Monday-Friday).

* AUP = <http://www.wheatoncollege.edu/policies/aup.html>

Here are some of the players in the intensifying battle over file sharing:



Sweden says it will criminalize peer-to-peer file sharing under the EU Directive, European Union Copyright Directive.

Of course, all these logos are fully-owned by their respective companies.

Protect Yourself from Digital Danger

Network Security: What You Need to Know Now

Wheaton's community depends heavily upon electronic services, from its business systems to electronic mail, to accomplish its mission. In support of that mission Wheaton's information services' objective is to maintain an open, collaborative and secure computing environment. There is an inherent conflict between open and secure; one that is difficult to balance. We have an obligation to provide accurate and reliable information to any authorized user.

Our electronic services are increasingly targeted by viruses, junk mail (SPAM) senders and intruders. We are working to protect our networked resources and want to keep you posted on our progress.

- **Viruses:** Information Technology and Services (IT&S) has taken steps to control viruses through central system monitoring and licensing antivirus software for all computers used by faculty, staff and students.

- **Junk mail:** IT&S is currently screening for junk mail and will continue to research the best practices for its control while being sensitive to the value our community places upon academic freedom and various points of view.

- **Intruders:** Intruders present the biggest challenge to the openness of our computing environment and to the viability of our electronic services and the critical information they house. Intruders routinely attempt to break into the central servers that run our electronic systems. If successful, they could damage or steal the information that is housed there or lurk, stealing passwords that could be used to access other campus systems and beyond. IT&S monitors Wheaton's servers, looking for suspicious activity. IT&S monitors national security alerts and constantly updates operating systems to respond to known vulnerabilities. In addition, IT&S is researching software and hardware solutions to decrease the risk from intrusions.

How You Can Help

You can help maintain our critical network and data assets by adhering to the college's Acceptable Use Policy (AUP), and by practicing good password management and protecting privacy.

Wheaton's Universal ID and Official Email Address

Why it's a good thing...
This change is the first step towards providing a single ID to log into all of Wheaton's electronic services.

What you need to do now...
You have already been issued a new official email address. You need to update your Webmail and/or Eudora settings.

If you need further information about these important changes please consult the IT&S homepage.

Acceptable Use Policy

Wheaton has policies regarding appropriate use of our networked resources. Your use of Wheaton's network indicates your acceptance of these policies; please be sure you have read them:

Students - <http://www.wheatoncollege.edu/policies/aup.html>

Faculty and Staff - <http://www.wheatoncollege.edu/policies/aupFS.html>

Good Password Management

1. Change your passwords frequently – once a month is ideal, once a quarter is OK ... anything less is dangerous.

2. Keep all your passwords private.

3. Until we are able to provide a more robust, single sign-on authentication environment, please use different passwords for the various Wheaton systems you access – Banner, email, Meeting Maker, Blackboard, etc. It is particularly important to keep your Banner and WINDOW passwords separate from your others given the sensitivity to the information housed there.

4. Use a combination of 8 or more mixed-case letters and numbers (where allowed) in your passwords to make them harder to guess (ex. sR38At01).

5. Never share your password or request it over the phone.

6. Do not allow a computer, or a service provider, to automatically save your password.

7. Do not make your passwords from any words or names, either backwards or forwards, that you can find in a dictionary – it takes only a few seconds for an intruder to throw a whole dictionary at your account.

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: http://www.wheatoncollege.edu/IT_S/email/. This can only be done while you are on campus or using a virtual private network client. For more information about Wheaton's VPN see: http://www.wheatoncollege.edu/IT_S/net/.

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.

Use Your Wheaton ID Card

Your Wheaton ID is now used to access Wheaton's many electronic resources, so you should take steps to protect it. Carry your Wheaton ID card with you. Use it when making routine transactions, such as checking out library books and eating in campus dining facilities. Please note: The barcode found on the back of your Wheaton ID card will still

Wheaton

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 three times a year, *Kaleidoscope* includes contributions from 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 contributions are welcome.

Marcia Grimes (*mgrimes*)

Jenni Lund (*jlund*)

Colleen Wheeler (*cwheeler*)

Network Security, continued

be needed to check out library materials, view your circulation record and use the patron self-renewal function in ELIZA.

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. Safeguard yourself and your personal information by clearing this information out of the browser's memory before you walk away from a public machine.

Here's how to clear your 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.

As always, please call the Support Center (x3900) if you need help with password changes or have any other computer support questions.

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 is compromised if you are sloppy about it. Remind your friends about this, too, since any sloppiness can make our entire network vulnerable to hackers who are looking constantly for weaknesses to exploit.

Good Habits

Do:

- Review and act on the "Good Password Management" section (this page, lower left).
- 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.



Network Security, continued in next column

Learn more on the IT&S web site at http://www.wheatoncollege.edu/it_s/.