

What You Should Know About P2P File Sharing

Information presented by these University of Tulsa units:
Center for Information Security
Enrollment and Student Services
General Counsel
Information Services

P2P file sharing applications such as Kazaa, Limewire and others have grown increasingly popular on college campuses. The primary application of these tools is to share copyrighted music and movies. Most users who engage in this activity are unaware, or do not fully appreciate, the legal and other risks involved. This document describes some of the hazards of using P2P applications and what you can do to protect yourself from these risks.

Copyright Infringement

Trading copyrighted works over a P2P network is engaging in copyright infringement. This form of piracy has mushroomed in recent years due to the proliferation of digital content and broadband connectivity.

The Recording Industry Association of America (RIAA) and many other organizations are seeking legal remedies and offering amnesty programs for the mass piracy occurring on P2P networks. In Spring 2003, the RIAA sued 4 students at 3 universities for copyright violations related to P2P networks. The RIAA (<http://www.riaa.com/>) and others are continuing this campaign by filing additional lawsuits against illegal file sharers.

The TU Ethics Code and Policy for Computer Use (<http://www.is.utulsa.edu/>) is clear on the matter of copyright infringement. The relevant text is plain:

“USERS MUST ABIDE BY ALL SOFTWARE LICENSES, TU COPYRIGHT AND INTELLECTUAL PROPERTY POLICIES AND APPLICABLE FEDERAL AND STATE LAWS.”

The University of Tulsa is compelled by law to act to stop copyright infringement on campus, and the University cannot shield its students or employees from copyright infringement lawsuits.

Impact on University Network Resources

P2P applications are commonly used to trade multimedia files between clients. Where such file trading is wide-spread, P2P clients can exhaust bandwidth and seriously degrade network performance. In some cases, P2P applications might install themselves on your computer as a super node, directing volumes of P2P search traffic through your system, all without your knowledge. If a disproportionate use of University computing resources is associated with your computer, you may be disconnected from the university network.

Security and Privacy

When you install a P2P client on your system, you are setting it up as a server. Remote users can access your shared folders and copy files from them. Configuring such a client improperly may result in sharing far more of your hard drive than you anticipated. A recent study (<http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf>) found that users can and do reveal sensitive information stored on their computers simply by misconfiguring P2P clients.

P2P clients expose your computer to all the security risks inherent to operating a server on a network. In a P2P environment, however, the risks are magnified by the limited defenses of the client and by the sheer number of users that can connect to your system.

Spyware is another threat. Spyware embedded in P2P clients (<http://news.com.com/2100-1023-257592.html>) can track your browsing habits and divert market-targeted advertising to your desktop or harvest personal information (e.g., your name and email address) to spam farms. Once spyware is installed on your system, it (by design) is difficult to remove, usually requiring additional special spyware removal tools.

Protection

You can protect yourself from these consequences and other hazards in a number of ways.

1. Do not use P2P applications to share copyrighted works.
2. Before installing a P2P client, investigate the known security vulnerabilities and spyware issues associated with it.
3. If a P2P client is installed on your system, disable file sharing or check the "Shared Folders" configuration to make sure your files and data are not unnecessarily exposed.
4. When you leave a P2P program, make certain to exit and close the server. (You should go to the "File" menu and click "Exit" when you leave a P2P program; do

not simply close it using the "X" in the upper right of corner of the window. Anytime you see a P2P program server icon in your system tray, usually in the lower right corner of the screen, right click on the icon and click "Exit" to close the server.

5. Do not install P2P clients on university computers without approval from the appropriate system administrator.
6. Contact Information Services at the University of Tulsa (x3500) if you suspect your system is experiencing problems resulting from the installation of P2P software.

By following these guidelines you can minimize your exposure to the risks associated with P2P networks.