



File-sharing and P2P

Stonehill College Information Technology
Help Desk 508-565-HELP (4357) helpdesk@stonehill.edu

File-sharing and Peer-to-peer Software Benefits and Risks

What is file-sharing and peer-to-peer software?

File-sharing involves using technology that allows internet users to share files that are housed on their individual computers. Peer-to-peer (P2P) software is any file-sharing software that allows users to both share content from their computers and to connect to other, similarly configured computers for the purpose of downloading content. Examples of this type of software include Kazaa, Bittorrent, Warez and Gnutella.

P2P file-sharing software has the potential to cause serious problems for your personal system as well as the Stonehill College network. Irresponsible file-sharing creates a tremendous strain on our campus network, interfering with other users' ability to connect to the Internet for academic and administrative purposes. In addition, P2P software is often configured so that other users can access your hard drive and share your files all of the time. Most of these also come bundled with "adware" and "spyware" applications, which allow third parties to monitor your Internet usage and send advertisements to your computer even when you are not using your file-sharing program. This kind of activity degrades your computer's performance and monopolizes additional network bandwidth. Finally, many files available for download are infected with computer viruses. Some viruses are designed specifically to spread through P2P networks.

File-sharing applications make it easy for you to share music, videos, movies, software, text and other files. However, unless you have the explicit permission of the copyright owner to possess or distribute the material, you may be in violation of federal copyright law. It is best to assume that all material is copyrighted. Sharing copyrighted files may also be grounds for enforcement action by copyright owners under the Digital Millennium Copyright Act.

Stonehill recognizes that there may be legal benefits of P2P software. However, the college is firmly against the unauthorized downloading and sharing of copyrighted materials. Installing file-sharing utilities could jeopardize the security of institutionally owned data and your own files. Therefore, it is important to learn about the proper use of the software, recognize the risks, and take steps to protect your computer.

What are the specific risks involved with file-sharing?

Installation of malicious code

When you use P2P applications, it is difficult, if not impossible, to verify that the source of the files is trustworthy. These applications are often used by attackers to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When you download the files, your computer becomes infected.

Exposure of sensitive or personal information

By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft.

Susceptibility to attack

Some P2P applications may ask you to open certain ports on your firewall to transmit the files. However, opening some of these ports may give attackers access to your computer or enable them to attack your computer by taking advantage of any vulnerabilities that may exist in the P2P application.

Denial of service

Downloading files causes a significant amount of traffic over the network and relies on certain processes on your computer. This activity may reduce the availability of certain programs on your computer or may limit your access to the internet.

Prosecution

Files shared through P2P applications may include pirated software, copyrighted material, or pornography. If you download these, even unknowingly, you may be faced with fines or other legal action.

How can you protect your computer?

Secure your peer-to-peer software.

Each piece of P2P software must be secured separately and often requires different security steps. The following are general security precautions you should take with each peer-to-peer network you use:

- Never reuse a password that you've used on a peer-to-peer network, because many of them don't encrypt passwords and your password can be intercepted much more easily from an unencrypted connection.
- Set your software to ask for your approval before a file is downloaded. This prevents virus-infected computers from automatically sending you more virus-infected files.
- Add the screen names of people you know to your IM, IRC, and chat-based peer-to-peer contacts lists, and accept only messages from people you know. Both viruses and spam are being broadcast to hundreds of chat-type peer-to-peer users at a time, and this helps reduce your computer's exposure to infected computers.
- **Partially disable uploading in your P2P application.** Doing this should NOT affect your ability to copy files to your computer from other locations. But it will prevent others from copying files from your computer.

Use virus-checking software

You're downloading files from unknown sources, so you must run antivirus software and patch your system regularly to make sure that your operating system is protected from any rogue or infected files you receive. Firewalls are still important, but because you've allowed the peer-to-peer software to access your computer through your firewall in order to share files, the firewall won't be able to block most peer-to-peer security attacks.

Turn off your computer

When you're not using it, shut it down. This ensures there is no unmonitored network activity originating from your computer. Several popular P2P applications run in the background even if you think you've turned them off. Turn off your computer so you don't have to worry about it, and you'll save energy too.

Turn off your P2P application

If you're using your computer, but you're not using your P2P application, make certain the application is turned off and not running in the background. Several P2P applications continue to run in the background even if you think you've quit the application.

Do not use automatic startup for P2P applications

Do not set up your P2P application to start automatically when your system starts. You may have done this when you installed the application. With this configuration you may not realize your P2P application is running and using system and network resources.

Queue your downloads

Queue your downloads so that only one file is transferred to your computer at a time. Consider all the other Stonehill network users – they need bandwidth too.

Download during off-peak hours.

Try to schedule file downloads during periods of low network use (weekends, early morning, late night).