DAS
DEPARTMENT OF ADMINISTRATIVE SERVICES
ENTERPRISE INFORMATION STRATEGY AND POLICY DIVISION

Enterprise Security Office Monthly Security Tips

NEWSLETTER

APRIL 2007 Volume 2, Issue 4

Security Concerns – Peer to Peer (P2P) File Sharing

From the Enterprise Security Office

Security Concerns Regarding Peer To Peer (P2P) File Sharing

Peer-to-Peer (P2P) networking has become a popular method for sharing files, music, photographs and other information. P2P allows computer users, utilizing the same P2P software, to connect with each other and directly access files from one another's hard drives. Napster was the original P2P program. Some of today's most popular programs are Gnutella, Morpheus, Kazaa, Filetopia, Limewire, Shareaza, and Bit Torrent.

Although the concept of file sharing seems benign, there are a number of risks associated with P2P.

Some of the major risks are:

- Sharing files on your computer with anonymous and unknown users on the Internet is contrary to the basic principles of securing your computer.
- Even if you know the source, in P2P, opening a file has risks – it may contain a Trojan horse, worm, virus or other malware.
- P2P may expose personal, private or confidential data on your computer.
- P2P software, like any other application, may contain vulnerabilities that could allow unauthorized access.
- It is possible that the P2P software may be a malicious version – it might include a virus or Trojan.
- P2P traffic may consume your bandwidth, diminish your computer's performance, cause a denial of service and impede access to the Internet.
- Some P2P programs may implement default settings that you do not want to use, such as scanning your entire drive, looking for files to share.
- Some of the files shared or downloaded may include copyrighted material, pirated software and other illegal material.

Because the negative effects of P2P far outweigh any potential benefits, the best way to protect your computer/system is to avoid P2P technology. In the event of a documented business case for using P2P, however, make sure a thorough risk assessment is completed before employing this service. If a P2P file sharing network is the only solution for your needs, consider the following tips for use of this type of service.

- Obtain explicit, written permission from your organization's information security group or IT director before installing a P2P client or using P2P network file sharing on a corporate network or system.
- Restrict access to those in your organization who have legitimate business needs for P2P file sharing.
- Obtain software only from known, legitimate and reputable sources.
- Restrict P2P access to only those folders specifically identified for this purpose. When you install P2P client software and join a P2P network, check to see if there is a default folder for sharing designated during the installation. If there is, limit file sharing only to this folder. The designated folder should contain only files that you want others on the P2P network to see and download. Be careful not to designate the root "C:" drive as the shared files folder; this would enable everyone on the P2P network to see and access virtually every file and folder on the entire hard drive.
- It is important that you have protective security software (anti-virus and anti-spyware) running on your computer. This software should perform a virus scan on any file you download before you execute or open it. Make sure

that the most current anti-virus software and virus definition updates are installed on your computer.

- Scan your computer periodically with virus and spyware detection tools to ensure you haven't installed malicious code on your system.
- Know the laws. There may be legal ramifications in sharing and/or downloading certain files. Downloading illegal copies of files (i.e. music, movies, etc.), downloading improper files on computers or networks, or sharing personal information may lead to legal consequences such as prosecution, disciplinary action or financial liability.

References:

Tips To Avoid Problems With P2P File Sharing
http://netsecurity.about.com/od/newsandeditorial1/a/p2psecurity.htm

P2P File Sharing Tips
http://onguardonline.gov/p2p.html

How To Disable Various P2P Software On Your Computer
http://security.uchicago.edu/guidelines/peer-to-peer/

Good and Bad Executable File Extensions
http://www.novatone.net/mag/mailsec.htm

US-CERT Cyber Security Tip ST05-007
http://www.us-cert.gov/cas/tips/ST05-007.html

Brought to you by:

MS-ISAC

http://www.msisac.org

DAS Users:
For **hardware and software issues**, contact the Technology Support Center at (503) 378-2135.
For **security issues**, contact the Enterprise Security Office at (503) 378-6557.