FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Division of Consumer & Business Education

P2P File-Sharing: Evaluate the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. To share files through a P2P network, you download special software that connects your computer to other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files – even giving access to entire folders and subfolders – you never intended to share. You may download material that is protected by copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- **Install file-sharing software carefully, so that you know what's being shared.** When you load a file-sharing application onto your computer, any changes you make to the P2P software's default settings during installation could cause serious problems. For example, if you change the defaults when you set up the "shared" or "save" folder, you may let other P2P users into any of your folders – and all its subfolders. You could inadvertently share information on your hard drive – like your tax returns, email messages, medical records, photos, or other personal documents – along with the files you want to share. And almost all P2P file-sharing applications will, by default, share the downloads in your "save" or "download" folder – unless you set it not to.

- **Use security software and keep it and your operating system up-to-date.** Some file-sharing programs may install malware that monitors a user's computer use and then sends that data to third parties. Files you download may also hide malware, viruses, or other unwanted content. And when you install a P2P file-sharing application, you might be required to install "adware" that monitors your browsing habits and serves you advertising.

  Malware and adware can be difficult to detect and remove. Before you use any file-sharing program, get a security program that includes anti-virus and anti-spyware protection from a vendor you know and trust and make sure that your operating system is up to date. Set your security software and operating system to be updated regularly. Make sure your security software and firewall are running whenever your computer is connected to the Internet. Delete any software the security program detects that you don't want on your computer. And before

you open or play any downloaded files, scan them with your security software to detect malware or viruses.

- **Close your connection.** In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. To be sure your file-sharing program is closed, take the time to "exit" the program, rather than just clicking "X" or "closing" it. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

- **Create separate user accounts.** If more than one person uses your computer, consider setting up separate user accounts, in addition to the administrator's account, and give those user accounts only limited rights. Since only a user with administrator rights can install software, this can help protect against software you don't want on your computer. It also can keep users from accessing other users' folders and subfolders, since users with limited rights generally don't have access to each other's information. Also use a password to protect your firewall and security software so no one else can disable them or grant themselves rights that you don't want them to have on your machine.

- **Back up sensitive documents.** Back up files that you'd want to keep if your computer crashes. Store them on CDs, DVDs, or detachable drives that you keep in a safe place.

- **Talk with your family about file-sharing.** If you're a parent, ask your children whether they've downloaded file-sharing software, and if they've exchanged games, videos, music, or other material. Talk to your kids about the security and other risks involved with file-sharing and how to install the software correctly, if they're going to use P2P file-sharing at all. If you're a teen or tween interested in file-sharing, talk with your parents before downloading software or exchanging files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.