

Shinn Technology Corporation

P.O. Box 173
Fishers , IN 46038

(317) 545-3650
<http://www.ShinnTechnology.com>



TITLE: Dangers of Online File Sharing

Due to the many questions that have come to attention, we are posting information about the dangers of online file sharing in an effort to make sure that our users have access to information we believe to be very important.

Online file sharing, otherwise known as peer-to-peer networking, allows users over a network (or the Internet) to upload and download files with their computers. In the past few years, a number of companies have produced peer-to-peer software in order to make it easier for the user to exchange files with other Internet users. Some of the well-known programs include:

1. KaZaA
2. BearShare
3. Gnutella
4. LimeWire
5. WinMX
6. iMesh
7. and many others

Many of these programs come with other "sub-programs" built into their software code. Some of these "extra" programs are designed to do a number of things, including:

1. Allowing popup advertisements to be sent to your computer.
2. Allowing "spyware" to run on your computer, which monitors where you go and what you do on the Internet; it also reports the information back to the designers of the software.
3. Taking control of your computer's unused processing power, and forcing it to conduct computing for whatever the designer of the software desires it to do.
4. Changing your computer's security configuration, which, in essence, can make it much easier for your computer to be taken over by another Internet user without your knowledge.

Many of these file-sharing programs are designed by inexperienced software developers, who release the program for users of the Internet to install. These users are often unaware that the software has not been fully tested to ensure the safety of the computer upon which it is installed. The following are just some of the reports that have been reported to our customer care center regarding "online file sharing" or "peer-to-peer networking" programs that caused issues related to their online security:

1. "Sleeper" software was found that makes the computer use its processor resources towards helping the software manufacturer render movie animations for the designer's financial gain, or for other business purposes.
2. Poorly written software code in the file sharing application makes it much easier for your computer to be "hacked" and controlled by another Internet user. Malicious people look for open ports (virtual doorways into your computer when online) that are caused by badly developed software code. Most users are unaware that they have been "hacked" until it is too late to do anything about it.

Not all hackers write viruses. Some hackers will take control of your computer without your knowledge, and then use your computer (and thousands of others) in a denial-of-service (DoS) attack against a website.

3. Software other than file sharing software was installed without the user knowing it. Most file-sharing creators will add other software packages inside them, and only by reading their very long User Agreements would a user have been notified about them.

Below is an example of "extra" programs that may be installed (along with the initial file-sharing program), as well as some of the very long and sometimes hard to understand User Agreements to which the user must agree when installing the software:

<http://www.kazaa.com/us/privacy/bundles.htm>
<http://www.limewire.com/index.jsp/faqs#sec2>

Even though these peer-to-peer networking programs do allow removal tools to keep from installing the "extra software," numerous online reports state that the program or computer on which it is installed are prone to "computer crashes" and other problems.

4. The file-sharing software downloaded by a user may actually be "hijacking" the way the user's browser works, as is described in this article: <http://news.com.com/2100-1023-864086.html>.
5. Hackers can write destructive viruses specifically for these file sharing programs, knowing that users are unintentionally spreading the virus over the Internet. Not only do users place themselves at high risk of receiving a virus when doing online file sharing, but others are also placed at high risk of infection, even without sharing the files using one of these programs.

Many viruses received through the downloading of "shared files" can infect your email client, thus infecting people you send emails to as well. You can receive detailed information about these types of viruses by going to Symantec's website at <http://www.symantec.com>.

6. Some software routines are very hard to remove when developers of file sharing software programs design a "software removal" program that will remove the file sharing application, but none of the "extra software" that is installed. There have been reports of users removing the software, only to have it "magically" reappear the next time they reboot their computer. One example of how hard it is to remove some of the peer-to-peer networking software is described in the following article:
<http://news.com.com/2100-1023-875274.html>.
7. Spyware programs not only violate the users' computer security by monitoring what they are doing, but also can cause slower Internet speeds and also generate large amounts of bandwidth on your internet service provider.

Shinn Technology Corporation discourages the use of file-sharing (or peer-to-peer) applications due to the higher security risks involved for our high-speed Internet users.