

# **Peer to Peer Networks – File Sharing gone wild, and dangerous**

## **By Jerry Williams (CIRJ Concepts)**

The largest audiences of the peer-to-peer (P2P), file sharing networks are those looking for “free music.” I have personally have renamed it “fee music” because there is a large price to pay if you are one of the unlucky ones.

We all know not to open emails or email attachments from people we don't know. Well, this is the same principle, but instead of receiving an email from someone you don't know, you are downloading directly from their hard drive. That's right; when you download that “fee music” you are downloading directly from someone else's physical hard drive and you have no idea that they may be sharing a virus with you.

A virus can easily be made to appear as a common file name. The ability to change a file name is a very basic computing skill. You click on the file and type over the name and you are done. This is what is happening with P2P networks (i.e. Limewire, uTorrent, BitTorrent, Morpheus and quite a few others). Malicious code writers are changing the name of a virus to your favorite song title and placing it in their shared directory. You download the “song” and now you have just placed a virus on your hard drive. Then, unknowingly, you share the same files/songs with others who put them on their hard drive. See how the cycle starts? This is one way viruses are able to spread rapidly through these P2P networks.

We have to remember that the Internet is also called the World Wide Web. Worldwide is the keyword. We never know where the content we are downloading comes from. With this in mind, we must take precautions to prevent malware and internet/email scams from harming you and your computer. A first good step is to no longer use the P2P networks. Another excellent step is to have active Anti-Virus protection. We recommend AVG Internet Security as it is the best we have found. You can contact us for information or to purchase. (We do not sell it to make money; we sell it because it protects you!) Another way to protect yourself is to adhere to the old saying, “if it sounds too good to be true, it probably is.”

### **What are peer to peer networks exactly?**

P2P networks are, in basic terms, file sharing applications. Examples are programs such as Limewire, uTorrent, BitTorrent, Morpheus and quite a few others. These programs work by allowing you to download files, videos, music, and software for no charge. You are sharing files with other users of the same application and this allows you to access their shared directory and download anything that is in there. The security alert is right there; you are accessing files on someone else's computer. You do not know if the file names are correct or if what they say they are sharing is truly what it is. Do you see the danger in this?

For example, if I wanted to spread a virus through a P2P network, which I don't, I would simply change the file name of the virus to a common song title such as DontWorryBeHappy.mp3. Then, after I place that file in my shared directory, you download the file thinking you are not going to worry and are going to be happy, but it turns out much different. You are forced to worry and happiness has evaded you. You have a virus or spyware loaded on your computer and all of your private information is at risk. Your computer may crash and you lose all of your precious memories and work or the virus sends all of your financial information to the persons who wrote the virus. Even worse, you may be charged with having child pornography on your computer but the file said it was a song? You were only trying to get a copy of a song you love? This is happening every single day; hour by hour. The danger far outweighs the benefits.

It has been documented that more than half of all files available for download from peer-to-peer networks have been deliberately infected with some form of malware (viruses, Trojans, key loggers, worms, etc.). Most P2P programs are set up to launch automatically at startup and are also configured to allow other P2P users on the same network to have open access to a shared directory on the computer. This is what makes you vulnerable to identity theft, data theft, and makes you instrumental in the spreading of various types of malware.

Peer-to-Peer networks are so dangerous to users and to various industries with copyright infringement, child exploitation and pornography, and computer hacking, that the FBI has issued a warning and launched an investigation into the use of these types of networks. For more information on the FBI's involvement you can visit the FBI website and read the posting at <http://www.fbi.gov/cyberinvest/cyberedletter.htm>.

The point we are trying to make is not to be so trusting on the internet. We have to use common sense when we are presented with offers for "free" things online. Unfortunately, there are too many criminals trying to take advantage of trusting people. We recommend uninstalling the P2P network you have and get rid of any content you have obtained through that network. After you have done this, you will want to run a thorough virus scan to be sure you are not infected. If you believe you are infected with a virus or other form of malware, please contact us immediately. Time is money with viruses. The longer they have to ruin your computer, the more it will cost to fix. We are experienced at correctly disinfecting computer systems and repairing any damage malware has caused. We hope we don't have to hear from you in this case only.

Should you need our assistance or have questions, please feel free to contact us at [Support@CIRJConcepts.com](mailto:Support@CIRJConcepts.com).

Author: Jerry Williams  
[www.CIRJConcepts.com](http://www.CIRJConcepts.com)