

## Peer 2 Peer Networks & Your Businesses Risks

By

Brian Wilson

CCNA, CSE, CCAI, MCP, Network+

[Slimjim100@gmail.com](mailto:Slimjim100@gmail.com)

[www.middlegeorgia.org](http://www.middlegeorgia.org)

[www.Middlegeorgia.info](http://www.Middlegeorgia.info)

(AKA Slimjim100)

As most of us had heard of p2p networks and services like Kazza and limewire what we don't think about is that businesses are responsible for the activities on there networks. When an employee, vendor, or customer is on your businesses network do you know what they are doing? Well for businesses like Hotels, Internet Café's, or Public Access Points you are at highest risk for users to abuse you network. You will need to restrict cretin activities or you will find you ISP terminating your service or worse getting sued from the RIAA or MPAA. For the rest of the business owners you might want to understand the risks of lax network security and the true cost you could pay. Employees might want to surf the internet when they are at break or though out the day. This can be fine if you have web filtering. Some issues faced with web surfing at work is that if an employee downloads or installs peer 2 peer software. The biggest problem with most peer 2 peer programs that 80%+ of the contend hosted in the networks is stolen copyrighted content or viruses. This means if the owners of the content notice the download your business is liable for the theft. Other issues are viruses and Trojan programs that might compromise your Businesses data.

Understanding the issues is the first step to preventing your business from liability. Most businesses that have avoided this issue are implementing Web filters, Network Security, and employee training. Some the of things you can do is make sure you have a firewall installed and understand the ports that peer 2 peer software uses and then you are on your way to blocking the software. Here is a list of the most popular P2P programs and networks. Hotels, internet cafes, public wireless spots, etc. should block these ports to avoid any copyright issues with the use of their internet access.

- \* BearShare, Mopheus, Limewire, Gnutella  
6346 and 6347 TCP, UDP
- \* Kazza, Grokster  
1214 TCP, UDP
- \* Autontp, BeNapster  
6699 TCP
- \* Napster, Duskter, Gnap  
6700 TCP
- \* Inapster, Jnap, WinMX  
6701 TCP
- \* Edonkey  
4661, 4662, 4665 TCP, UDP
- \* iMesh  
4329 TCP

The above listed is just some of the most common peer 2 peer network software & ports. It is always recommended to consult you networking vendor to insure you have the most up to date software and hardware to protect you business. In addition to port blocking there are other things can do to help you businesses network. Impose network policies for all users and keep all you network protection software up to date (Anti-virus, Spyware, Ad blockers). Provide Training to you users to explain the risks of the internet. One of he biggest risks to business networks are the users and the only way to insure network safety is to make sure the users fully understand network policies. Once your users have an understanding of the risks online and fully understand there responsibilities as a network user. You are that much closer to a safe digital work place. As always most local network consulting firms can provide what I have discussed and you may need to take additional step to meet the needs of your business. With HIPPA and Sorbian Oxley there is no reason to risk liability on your company's networks. As we see in the media every day more and more businesses have been learning the hard way about corporate liabilities.