P2P or Peer-to-Peer Safety, Privacy and Security

What are the *Other* Risks?

Most articles about the risks of P2P focus on piracy and copyright issues. Few have taken the time to explore other risks the technology poses and solutions to those risks. In addition to traditional P2P technologies, such as Kazaa, eDonkey and Morpheus, many of the new instant messaging technologies have P2P features and allow the sharing of files, even very large media files, such as videos. While both P2P and, more obviously, IM applications with P2P feaures have many benefits, like most other Internet-related services and applications, there are risks. Luckily, there are solutions for most of these risks if you know what to look for.

Since it was first launched a few years ago, P2P has been demonized for facilitating music, movie and software piracy. But putting the piracy issues aside for the purposes of this article, what are the risks associated with using P2P in a home and in a business or school environment? These risks include 1. infecting your computer with malicious codes, such as viruses, worms, Trojan horses, spyware and unwanted adware, 2. illegal, harmful and child-inappropriate content, 3. making your computer more vulnerable to hacking and other intrusions, 4. allowing others to make your computer into a drone capable of attacking other websites and servers, 5. corrupted files or misrepresented content and 6. sharing private files, unintentionally, with others. There are ways to avoid these risks, if you are forewarned and use the right software and security precautions.

These same tips apply to IM P2P applications.

Malicious Code:

According to leading computer security experts, viruses are very prevalent in P2P networks and are expected to grow in P2P networks. One study concluded that 45% of the files found by popular keyword searches were infected with viruses.[1]

Trojan Horses and other hacking programs, Spyware and Adware are a growing problem as well. Many of the P2P applications include spyware and adware applications. And most inform the user that they contain such applications in their terms of service, license or privacy policies. But few people ever read those disclosures before clicking “I accept” and have no idea they have consented to the installation of spyware and adware

---

[1] Bruce Hughes, director of malicious-code research at TruSecure Corp.'s ICSA Labs, set up a search “on Kazaa and other peer-to-peer networks, scanning for popular file types using keywords such as sex and antivirus. Hughes says 45% of the files he downloaded contained malicious applications. "If you're downloading files from these networks, you're going to get infected with something," he warns.”

programs. Some files, disguised as MP3 files or other downloadables are really hacking Trojan horse applications which give their users access to your computer remotely.

While laws are pending in various states and federally, the best way to protect yourself against unwanted spyware and adware applications, as well as hostile code such as Trojan horses, is by using a good anti-virus program updated automatically. The addition of a firewall (either software firewalls or hardware/router firewalls) can give you the protection you need against intrusions. Make sure that your software applications work on IM and P2P programs.

Some of the more popular P2P programs offer premium services for a fee. These premium services are warranted to be virus and malicious code-free, and often promise not to include any executables, such as adware or spyware applications. Many people (especially parents) confuse the fee for the ad-free, spyware-free and virus-free service for a license fee for music or movies available on the P2P network. They believe (wrongly) that they have now paid for the right to download music and other media. This is one issue that might require action by the FTC or state consumer protection agencies to clarify. I recommend that the P2P premium services make it clear what the fee is and is not for, to avoid consumer confusion. Some of the more nefarious companies and websites intentionally mislead consumers into believing that they are paying for the right to download music and other media, when they pay a fee for the P2P software application the more responsible networks provide without charge.[2]

Illegal, Harmful and Child-Inappropriate Content

Child Pornography is, unfortunately, a serious problem in P2P networks. It's an easy way to transmit larger media files, which often include videos and still images of children being molested. And help groups, such as WiredSafety.org and others, are unable to search for child pornography since to view a file in a P2P setting, you must download it to your own computer. Downloading child pornography, saving it in any format, copying it or otherwise transmitting it, are all serious crimes in the United States.

The P2P networks are now very active in trying to stem the distribution of child pornography and child exploitation files. They have, in recent years, worked very closely with law enforcement agencies and have willingly cooperated in investigations to stop and prosecute child pornographers. They are now important partners in the worldwide fight against child exploitation.

Sadly, in the early years of P2P this wasn't the case. I had personally contacted several P2P networks (thankfully, none of which are still in business) with child pornography I

[2] Similar schemes are used by identity thieves to collect your credit card information. They promise you that you can download first run motion pictures and software applications at a reduced cost or for free, once the application or website access is paid for. They collect your credit card information, but never charge it themselves. The "too good to be true" movies or software never arrive, but the consumers don't worry about it, since the website didn't charge them. Instead, they sell it or otherwise provide it to others who *do* charge it, fraudulently.

discovered while representing a famous pop-star. I was retained as her counsel in an attempt to stop fraudulent pornographic images of her from being posted online and in P2P networks. The network executives refused to return my calls and refused to take down the images. They only cooperated when law enforcement became involved.

Unfortunately, few child pornography images are caught by filtering software programs or parental controls. Most of these products work using either known lists of images or textual descriptions or names of images. Typically, child pornographic images do not use the words or names that would otherwise trigger a filtering product.

The only way to avoid child pornography on P2P networks is to steer clear of search terms that might imply images of young children or preteens. Even then, downloading unknown images can be risky.

Although some files provide an indication of their child pornography subject matter, using searchable terms such as “Lolita”, “young boys”, etc., the more sophisticated child pornography traders use other file names to mask their true content. It is possible for someone to innocently stumble across one or more of these files, while looking for other content. If anyone comes across a file they believe to be of child pornography, they should notify the P2P network administration immediately. They should not forward the file to anyone, print out copies or save the file to their computer or any other media. They should also contact National Center for Missing and Exploited Children’s Cybertipline, at www.cybertipline.com, noting the exact file name and location where the file was found. WiredSafety.org’s anti-child pornography campaign is “Don’t support it, report it!” If everyone reports what they find (without actively seeking it), the Internet will be a better place.

While P2P networks contain many violent, hateful, pornographic and other potentially harmful content files, they are largely not illegal in the United States. But they may be offensive to many adults and highly inappropriate for children. Most of the parental controls and filtering software programs now filter all content downloaded from P2P networks. In addition, most popular P2P networks have premium services available for a fee that provide content filters.

Given the content issues, as well as the risk of exposing private files to the public by using the wrong settings for shared files, P2P is not appropriate for preteens. The best choice for parents of younger children, especially preteens, is to prevent your children from using P2P networks entirely. If there is a file they need for school, or otherwise want, the parent can access it for them. This would also have the added benefit of keeping the children from pirating music, movies and software when they may be too young to appreciate the ramifications of their actions. For parents whose children may not listen to their rules, many parental control and filtering products have settings that would allow parents to block their children’s access to P2P networks and prevent them from downloading the P2P software applications.

Security and Privacy Risks

Files subject to sharing:[3]

Private and, in some cases, very sensitive files, are often shared inadvertently by people using P2P networks. A study was done by HP and the University of Minnesota on P2P file sharing to test how prevalent inadvertent file sharing was on the P2P networks (http://www.hpl.hp.com/research/idl/papers/kazaa/index.html). In a survey of 12 users, only 2 understood what files were subject to sharing. This is particularly alarming because of the kinds of files they discovered were being shared, undoubtably, without the user's knowledge.

In a test conducted, searches for Outlook database files were conducted every 1-1/2 minutes for a 12-hour period on Kazaa. The study showed that many people had made private files open for download by others on the P2P network. These files include financial information, e-mail files and even browser caches, showing others where the user had surfed. Many people are not aware of how to limit the files that can be accessed from the P2P network on their own computers. And with the ease of P2P file search, others who understand what to look for can easily find these private files. The same study showed that on a dummy server set up with files identified as creditcard.xls and outlook databases, four unique users downloaded these files during the test 24-hour period. So, not only are users making their private data available to others online in P2P environments, but others know this and search for and download these files.

This tells us that we need to be sure what files are subject to sharing, how to make other files subject to sharing or stop sharing of those files, how not to make mistakes when we allocate files for sharing and understanding the import of the data contained in files to be able to determine the risk of sharing them.

The more sophisticated P2P purveyors use a wizard or user-friendly interface to help the user locate the shared file folder and limit the risk of sharing private files unintentionally. But if the wizard is by-passed or the default settings modified, or the wizards are not created with the user's privacy in mind, the potential for mistakenly sharing files is very real. Selecting a new location for downloaded files broadens the files subject to search, scrutiny and download by others in P2P. All files located within or under a specified file

---

[3] "The results of 443 searches in 12 hours showed that unintentional file sharing is quite prevalent on the Kazaa network. 61% of all searches performed in this test returned one or more hits for inbox.dbx. By the end of the 12 hour period 156 distinct users with shared inboxes were found."

"To further demonstrate that this indicates unintentional file sharing, we examined 20 distinct cases of shares on the inbox.dbx file by manually using the "find more from same user" feature. 19 of the 20 users shared the other email files found in the default Microsoft Outlook Express installation (Sent Items, Deleted Items, Outbox, etc.) In addition, 9 users had exposed their web browser's cache and cookies, 5 had exposed word processing documents, 2 had what appeared to be data from financial software and 1 user had files that belong in the system folder for windows."
Quoting: *Usability and privacy: a study of Kazaa P2P file-sharing*, Nathaniel S. Good, Information Dynamics Lab HP Laboratories and Aaron Krekelberg, Office of Information Technology, University of Minnesota.

folder are also available to others for searching, scrutiny and download. This is not very clear to the typical P2P user.

Gathering information about operating system to determine vulnerability:

If you have permitted file sharing, others may have access to your system and your IP address. The more any potential intruder has about your system, the applications you use and the hardware settings, the easier it is for them to hack into your system and through your system to the network at work or the school network servers. And, as a rule, the longer your system is open to others, the easier it is to hack.

Even if you aren't aware it is running, it may be running in the background. A good rule of thumb, if you want to share files with others at all, is to shut down file sharing when you are not actively downloading or permitting others to download from you. That sounds far easier than it really is, however. Each P2P application has different ways of turning off file sharing. And these may change from one version to the next of the same application.

Cooperative networking

In addition, P2P applications can be a huge drain on bandwidth and system resources and can expose the system/computer owner to legal liability for illegal content (such as child pornography) or pirated content housed on the servers or computer. Many experts believe that they provide the potential for amassing large networks of computers for cyberterrorism and cybercriminal motives. They cite to several cooperative networking projects, such as the one to find life in outer space operated by SETI and another to break encryption codes, as proof that this kind of networking is possible and easy to create.

General advice for parents, employers and school network administrators:

You have the right to know what is being installed on your computers and networks. You should start by setting rules about what can be used and what can't and how permission can be obtained for installing new software applications. Rules should also be set for running all programs and files through an automatically updated virus blocker before they are installed on your computer. Parents should make sure that no software is installed without their permission.

But with P2P and IM programs, you may need protective software more than ever. These should include an adware blocker or removal program, a firewall[4] and an anti-virus program.

[4] Hardware firewalls are physical devices plug into the network. They are often safer, faster, pre-configured and should be able to protect the entire network. Hardwire firewalls, often costing hundreds of dollars, are also much more expensive than their software counterparts.

Often consumers (and even some network administrators) don't understand which security applications and hardware they really need and frequently confuse one with the other. An anti-virus product will review files that you intentionally download or install. But a firewall will keep out intruders and attempts to install something without your knowledge. They work hand in hand, like good brakes and seat belts. You are not fully protected unless you use both. Firewalls can be either software or hardware. They are also often included in wireless routers and in cable routers, for broadband users. So, check to see what you already have before you spend money to buy something you don't need.

Having the software and using it correctly are very different, though. Using the wrong settings, or disabling it because it takes too long to load, can leave you wide open to malicious code and hacking attacks. Read the directions that come with your products carefully, and ask the company's help desk or seek understandable information from their site if you have questions. If all else fails, ask your eight-year old for help. They are the cheapest computer experts I know that still do housecalls.

A software firewall is an application that runs on a computer, which tries to protect the computer that it is installed on. A software firewall may slow down the computer, and may not offer any protection at all if not installed and configured properly.