

Safety Tips for Peer-to-Peer (P2P) File-sharing Services



Peer-to-peer (P2P) file-sharing services are a popular tool that enables young people to share media files such as music, movies, or video games with their peers. The power and popularity of these free services lie in the ease with which this type of sharing is done -- by enabling users to connect to a network where they can access shared files residing on the computers that are part of the network. Peer to peer networks are a revolutionary way of distributing your own personal files like photos or songs. But while there are legal and safe ways to use P2P networks, young people may want to consider the following risks before using them.

Peer-to-peer (P2P) file-sharing: swapping music or other files on peer-to-peer networks which connect millions of people. Users download P2P software onto their computer to link them to the network and give them access to shared files, from shared folders on their hard drives. The more advanced "BitTorrent" network has made file-sharing quicker by enabling users to download chunks of a file from different users all at once. This means that each hard drive is accessible by all other users of the P2P network at that moment.

Know the Risks

There are two categories of risks to consider when using P2P services: the content that can be accessed and the security of the service itself.

Content Issues

Most of the public discussion and concerns about P2P services have centered on the legal issues, namely copyright infringement and the age-appropriateness of the media being shared (pornography or violent games). The files that young people share may be pirated material and the distribution of

these files may be illegal. A young person may or may not be knowingly engaging in the illegal behavior. Regardless, they may put themselves or their parents at risk of breaking the law.

Young people should consider the following questions when using a file-sharing service:

- **Is the file I want to access really what its name indicates?**
Sometimes files available through P2P sharing sites have names that are deceptive and even files named 'Winnie the Pooh' or 'Pokemon' have been found to contain pornography.
- **Is the file a legal copy of a CD, DVD, or video game?**
While it may not be easy to determine if a file has been pirated, young people may be sharing files they know have been illegally copied.
- **Does the file have limits on distribution?**
e.g. You can make a copy of it, but only for yourself, not someone else.

If a young person is uncertain about the answers to any of the above questions, it is best to advise them not to download or share the file.

Security Issues

File-sharing services have also increasingly become a destination for cybercriminals to fool people into downloading fake or malicious software, using both overt and covert techniques. A young person should be aware of offers for discounted security software or links to third-party sites with "deals" because these may be techniques designed to trick them into downloading bad things that can cause harm later, a tactic known as "social engineering".

Likewise, a young person may leave their computers vulnerable due to the openness of P2P networks. Cybercriminals drop copies of malicious software into shared folders of popular P2P file-sharing applications, using enticing names

for the software so that as many as people as possible will download it. Once a computer has been infected with this kind of software, any number of things can happen to it. Depending on the intent of the cybercriminal, they can steal information using methods such as capturing screenshots while the computer is in use (which may contain personal information) and sending that information back to the criminal.

Be Prepared

A combination of awareness of what is legal and what isn't, proper use of the file-sharing service, and security technology can help young people safely and securely enjoy sharing their favorite forms of media with their friends using P2P services.

Below are some tips that parents can share with their kids so they stay safe while enjoying the benefits of file-sharing services:

1. Only use legal file-sharing services.

If you want to stay on the right side of the law, there are a number of legal downloading sites with music and other media that allow you to enjoy media without fear of being prosecuted. Different services have different terms - for example, some give you unlimited access to the content you purchase, others limit the number of compilation CDs or DVDs you can burn. Some let you pay per item, others charge a monthly fee. It's a good idea to look around the Web and see what works for you.

2. Be alert when installing file-sharing software.

It is easy to rush through installation screens when you really want to hear a new tune or see a film, but it is important to think about whether you want to share as well as download, and what other content on your computer might be vulnerable if you choose to share. When you are installing the software, check the Options or Preferences and read each screen before clicking "Next" to make sure you're not accidentally sharing your private content with the outside world.

3. Check the user comments feature of your file-sharing software.

P2P files are not always what they are labeled to be. If you are using file-sharing software to download music or movies, you may come across files that are not named correctly or contain material you were not expecting. Most programs have a ratings or comments system in which users who have downloaded the same file can report on whether it was what they expected. It is a good idea to check this before you start downloading - and to participate in the system to help other users.

4. Talk with your kids about what is appropriate media for them to hear, see, or use.

Deciding what is right for your kids to be exposed to, online or off, is a personal decision. Kids will have access to a lot of content once they are online, but it is your guidance and their own critical thinking that can help ensure they are not exposed to anything that is inappropriate for their age or may be harmful to them in any way. Some of the files they may try to access may also be infected with malicious software, so teaching them to think twice before downloading something they think may be questionable is a good skill for them to learn.

5. Make sure you have up-to-date security software on your computer.

Even if you do all the right things, cybercriminals are using more stealthy ways to load malicious software onto your computers. A popular way of doing this is through file-sharing services. They attempt to hide or disguise this kind of software by burying it into a legitimate video or music file. With security software installed and up-to-date on your computer, you can better ensure the security of your computer and all you have on it.