



Factsheet 13 – Understanding and reducing security risks associated with peer to peer file sharing

What is it?

Peer-to-peer is a term that is commonly associated with “file sharing”. Peer to peer (P2P) file sharing is popular among home-based Internet users but many home users are not fully aware of the security issues surrounding the use of P2P services.

P2P file sharing occurs between ordinary¹ computers (peers) connected to the Internet and between people who generally do not know each other around the world. Typically, the types of files shared are music files, movie files, TV shows, computer games and other software – both free and proprietary. While P2P file sharing can be used for legitimate purposes, generally, much of the content shared includes copyright protected material and is generally being shared illegally, that is, in breach of the copyright licence.

The purpose of this Factsheet is not to discuss the legal issues or risks, but rather to highlight the security risks P2P file sharing poses to your computer and personal information.

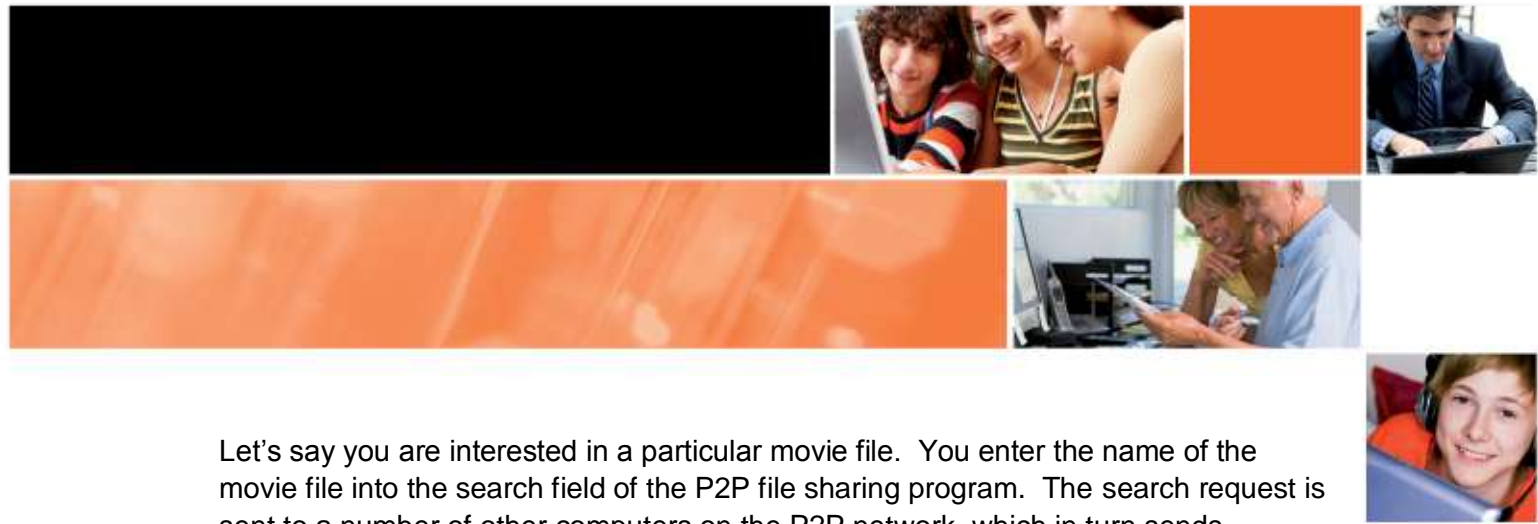
How it works

To participate in P2P file sharing you must install P2P software on your computer. Commonly used P2P file sharing software includes Shareaza, BitTorrent, BearShare, Kazaa, Limewire and eMule.

Downloading – requesting copies of files from other computers

Once P2P file sharing software is installed, your computer automatically becomes part of the P2P file sharing network. You can then search for copies of files of interest to you on other computers that are part of the network.

¹ Ordinary computers are those used by people, such as the computer being used to read this Factsheet. It may be a laptop computer or a personal computer used at home or work.



Let's say you are interested in a particular movie file. You enter the name of the movie file into the search field of the P2P file sharing program. The search request is sent to a number of other computers on the P2P network, which in turn sends requests for the movie file to other computers on the network.² The results of all the searches are sent back to the requesting computer. Depending on its size, the file may be broken down into parts where no single computer has a whole and complete copy of the file. Rather to get a complete and usable copy of the file your computer then connects to the multiple computers where the file fragments are located and begins to copy (download) them to your computer. When all fragments are copied (downloaded) to your computer they are reassembled into a single usable file.

Uploading – sharing copies of your files

Conversely, other people with P2P file sharing software can search your computer for files or content you have on your computer that is available for sharing. If a match is found, a copy of that file is sent from your computer (a peer) to the computer (a peer) of the person who requested the file. Depending on the type of P2P program and how it is set up, you may automatically share all the files you download or all the files in a particular folder.

Security risks

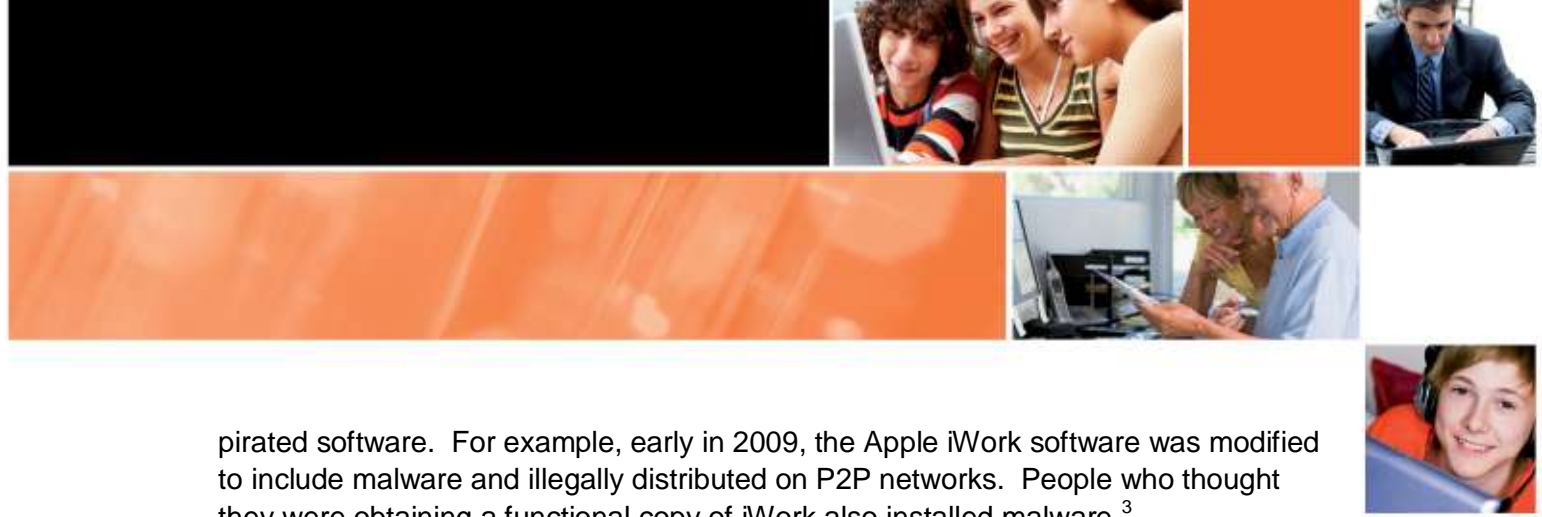
The nature of P2P file sharing allows anyone to connect to any computer (on the P2P network) and share anything they want to. This introduces security risks because neither the content being shared, which includes a lot of "pirated" (copyright infringed) content, nor the computers (peers) that make up the P2P network, come with quality assurance guarantees.

Malware

Any content obtained via a P2P file sharing network, including well-known software, documents, movie and music files can be embedded with malware that secretly installs itself (without the user's knowledge) when the file is opened.

It is common for fake and illegal software to be distributed via P2P networks. Often the software is modified to include extra malicious functionality. Unsuspecting users' computers could be infected with malware while installing and running the modified

² There may be some variation in how the searches are performed between different P2P file sharing programs and networks. In some cases the search request is sent to a centralised server, which monitors the file sharing content of the peer computers and reports where copies of the files can be obtained back to the requesting computer.



pirated software. For example, early in 2009, the Apple iWork software was modified to include malware and illegally distributed on P2P networks. People who thought they were obtaining a functional copy of iWork also installed malware.³

This is a common strategy used by criminals which allows them to take control over these computers. Once these computers are compromised and in the control of the criminal they can be used to support a range of other criminal activities, including stealing your personal financial information and passwords, among other things.

Leaked personal or sensitive information

Another major security threat is the accidental leak of sensitive documents and personal information. When setting up P2P software, it often sets up a publicly visible share of your files for others to access. This has resulted in the leak of sensitive government documents as in the case of the blueprint for Obama's helicopter.⁴

Network slowness

By making your computer part of a P2P network, you automatically increase the amount of bandwidth you use. Even when you are not downloading P2P content, your computer may be uploading copies of files from your computer to other computers. The process of uploading will degrade the overall bandwidth available to you to do other things online, regardless of whether the upload is included or excluded from your monthly quotas. Hence, if you have P2P file sharing software installed and find your network connections are unsatisfactorily slow – this could explain why.

How to reduce your risks

Home users

1. Unless you are an experienced computer user with a superior ability to manage security risks, most forms of P2P file sharing is risky. The best way to reduce your risk is to avoid installing and using P2P file sharing software, thereby preventing P2P file sharing networks from having access to your computer and files. If you already have installed P2P file sharing software, then you can reduce your risk by uninstalling the software.

³ See the media release from Intego at <http://www.intego.com/news/ism0901.asp> for more information.

⁴ <http://news.cnet.com/data-about-obamas-helicopter-breached-via-p2p/>



2. If you previously had P2P file sharing software installed, but since removed (uninstalled) it, check that it did not leave open P2P ports on your computer and created holes in the software firewall and/or modem/router, which allows others in the world to covertly and remotely access your computer.
3. If you choose to continue to use P2P file sharing networks, check that your P2P file sharing software is set to enable you to download files but not upload or share files with others on the network.
4. If you choose to also share files, check which directories are marked to be shared to ensure that only information you want to share is actually being shared.
5. Also, to reduce the amount of bandwidth used (in terms of uploading), turn the computer off when you do not wish to use it yourself.
6. If downloading files from the P2P network, scan the files with a good quality anti-virus program before opening the files.
7. Apart from these specific issues, maintaining good security on your own computer will reduce the chance that you will become infected with malware inadvertently installed or passed to your computer. This includes following all steps in the [Secure Computing Checklist \(Factsheet 1\)](#). Bear in mind that connecting to P2P networks increases your risk of exposure to malware at the same time.

Small to medium size businesses

1. If you run a small or medium size business, it is good practice to have computer security policies which explicitly disallow the installation of P2P software on computers on your network.
2. Besides the security and legal risks, another good reason to prohibit the use of P2P file sharing on your network is that P2P file sharing often consumes huge amounts of bandwidth – both into and out of the network. This can add considerable cost to the business and depending on the business, potentially reduce the bandwidth available for critical business services for customers and employees.
3. Configure your firewall to block connections inwards and outwards from hosts that use common P2P ports.

Report prepared May 2009