

Network Box White Paper: Securing social media series

Part 6: Peer-to-Peer

What is peer-to-peer?

Peer-to-peer (P2P) technology allows networks of people to share access to digitally stored files, such as music and video. Having been made popular initially by Napster in the late 90s, it has been back in the spotlight recently with high-profile legal action against services such as Pirate Bay and Kazaa, and their equally high-profile come-backs (<http://news.bbc.co.uk/1/hi/technology/8159560.stm>).

Younger consumers particularly use P2P and file sharing sites to download music (often illegally). But it is not just the realm of the young; increasingly, P2P services such as BitTorrent are used to download films and music (even Stephen Fry was reported recently to have used BitTorrent to download an episode of House <http://www.guardian.co.uk/media/2009/jul/13/stephen-fry-hugh-laurie>).

There are a number of P2P networks, software providers and applications. P2P networks, such as Gnutella, or the soon-to-be resurrected Pirate Bay and Kazaa, work by their users downloading software that lets them connect to a P2P network, and search and download files stored in shared folders on other network users' computers (using them as servers). Files are transferred between members over the Internet.

BitTorrent is a protocol for downloading and distributing files from a network. It works by dicing up media files into small 'pieces', pulling together these pieces from different parts of a distributed network to provide a whole media file (film or music). Dicing media up like this means that the user can start playing the first 'piece', as the remaining pieces are being downloaded, which reduces the time lag between starting to download a file and being able to play it. As a user downloads a piece and views it, they are simultaneously uploading it to another user requesting the same media file. This reduces the bandwidth required for a user to upload a shared file, as only a small chunk of the file is being uploaded from a single user's computer.

How does it work?

Broadly, P2P technology works using a port on your computer to allow data to pass to and from it, via the Internet which normally requires a change to either local or company firewall or both. It installs software that communicates with other computers to find and download the material you request.

Is it legal?

The technology that allows file-sharing is legal, if it is put to legitimate use. It is the downloading of copyrighted material (such as films or music) that is illegal, rather than the technology or process used to do it. So whether the service is legal or not really depends on how it the technology is used. SoundCloud, for example, is a legal service that was developed for the music industry, to allow users to share large music files where they own the rights to distribute and play it <http://venturebeat.com/2009/04/16/soundcloud-raises-33-million-for-audiophile-file-sharing/>. However, the cases brought against Pirate Bay and Kazaa – both now in the process of re-launching as legal, subscription-based services <http://blogs.wsj.com/digits/2009/07/22/the-pirate-bay-kazaa-attempt-to-relaunch-legally/> - demonstrates how P2P services can fall foul of the law.

There are a other legitimate reasons for using P2P as it helps to speed up the distribution of files and applications. For instance, some companies distribute updates to their operating system through P2P to reduce the load on their servers, increase resilience and improve download times.

Some ISPs (notably Eircom) have agreed to block certain illegal file sharing sites <http://www.computing.co.uk/computing/news/2237004/ireland-largest-isp-block-file>. The Digital Britain report produced in July 2009 has tasked ISPs with reducing illegal file sharing by 70 per cent within one year, monitored by OfCom <http://www.guardian.co.uk/technology/2009/jun/16/filesharing-digital-britain>.

What are the security risks?

There are a number of serious risks to using, or allowing employees to use P2P technology. The main risks include:

An open network of users can access your PC. This has obvious associated risks. If you are part of an open file-sharing network (ie. not a network created for and secured by your company), there will be any number of people you don't know accessing files on your computer. If vulnerabilities are found in the software you are using, you can expect them to be exploited. Added to which, files that have no business function may be using company resources (both hard disk and bandwidth) which reduces performance and the return on investment that the company might expect.

Downloading a P2P application onto a corporate network could expose corporate files. When you use a P2P network, you should limit access to a discrete folder containing media to be shared. However, the reality is that this relies on the user to ringence the media folder – if they don't, they could be opening up the entire corporate network to unknown P2P users. This has obvious implications for data and information protection.

The threat of malware. There are a number of ways that P2P technology could open you up to attack. In some cases, users may be asked to disable part of the firewall to allow file sharing – this has obvious security implications. The very nature of P2P files means that they are often not from a legitimate source. The user may be opening ports that they aren't aware of, and which can then be used by a hacker to:

- access personal data that could lead to identity theft
- 'plant' malware / spyware on the user's computer. This could be used to install software on a user's computer or exploit a flaw in the P2P application to allow a hacker to cause damage or access confidential company information at a later date, for example)
- take control of the computer and use it to distribute spam or malware (as part of a botnet); and download malware.

Creating network problems. The P2P application or software itself is likely to have been developed with consumers in mind, and may have inherent vulnerabilities that cause network problems.

Lack of anonymity and privacy issues. Often, a user's IP address is identifiable by other network users, which has associated privacy issues. If a user with malicious intent spots a corporate IP address in the network of users, they may decide to target that user to gain access to their corporate network

Bandwidth issues. Not only is bandwidth use a hard cost to the business, but downloading and uploading large media files to a P2P network could seriously impede network performance and hence employee productivity.

What should companies do?

There are very few reasons for allowing P2P technology onto the corporate network. Don't let employees download P2P software, or access P2P applications unless there is an explicit business reason for doing so. To stop employees doing this without your knowledge, you can:

1. Block outgoing, as well as incoming, data to prevent applications such as BitTorrent being used to distribute files
2. Monitor bandwidth use closely, by user. If it is unusually high, check that no media files are being downloaded, or uploaded by that user. Check files both entering and leaving the corporate environment
3. Monitor network connections closely. Only allow authorised applications to be used, ensuring all other ports are secured.
4. Keep your security systems up to date to ensure that any vulnerabilities are patched, and computers are scanned regularly
5. Ensure that any mobile devices (netbooks, laptops etc) that are removed from the corporate environment – for example, for home-working, or remote working – adhere to the same rules as those within the office. They should not be used for file sharing and should be using the most up to date security. It is critical that all devices used for remote working are secured in the same way as those within the corporate firewall. This will help avoid the situation where a child, for example, might use a parent's laptop to download music without their parent knowing. The same rules apply to home computers that are used regularly for work
6. If for any reason, file sharing is allowed on the corporate network, only use a legal, checked service. Specify what this service should be and only allow access to it. Talk to your security provider about checking that the service is secure, and ensure users:
 - a. Scan everything before it is downloaded onto the network
 - b. Set the default shared file to a closed drive. This should only contain files that you want others on the network to be able to view. Don't designate the 'c' drive as the shared drive – this could let everyone on the network see and access an entire hard drive, including operating system files
 - c. Know what they're downloading. It might be malware
7. Educate employees on the risks of using P2P networks and technology. Include this technology in your company security policy and ensure that employees are kept up to date as technologies change. At Network Box, we always recommend that companies hold an annual seminar on security to explain to employees what is, and what isn't acceptable at work. We recommend including the use of file-sharing and P2P networks and technology within this seminar.

For the latest security information, visit www.network-box.co.uk, or read Simon Heron's blog at <http://blog.network-box.co.uk>. You can also follow Simon on Twitter at <http://www.twitter.com/networkbox>.