

# P2P FILE sharing

What's illegal, what's at risk, and how to stay safe.

## what is P2P?

File sharing is a method of distributing electronically stored information such as digital media including movies, TV shows and music. One of the most common file-sharing methods is the peer-to-peer (P2P) distribution model.

P2P applications, such as BitTorrent, are legitimate and efficient software for sharing files but, like any software tools, they can be misused. Unfortunately P2P applications are used to share copyrighted materials including movies and TV shows without the express permission or authorisation of the copyright owner.

It has been estimated that over 1 billion searches are carried out daily by criminals searching P2P networks for sensitive and personal information stored on personal computers.

([www.netsecurity.org/secworld.php?id=5808](http://www.netsecurity.org/secworld.php?id=5808))

## what are the dangers?

As a user of P2P software, you may well get more than you bargained for when you install a program with the purpose of sharing files.

### P2P Application Security

Many P2P applications automatically share files back onto the network to increase the amount of files on the network available to its users. This data often is set to come from your "Documents" folder where your personal information may also be stored. With this information available for others to see and access, it is possible someone could use this information to steal your identity.

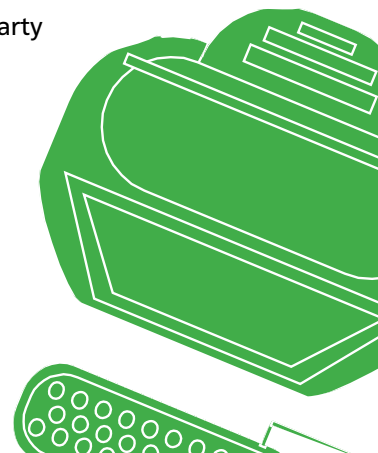
### Viruses, Worms and Trojans

Viruses, Worms and Trojans can be collectively referred to as 'malware'. These small programs which are often distributed with files shared on P2P networks,

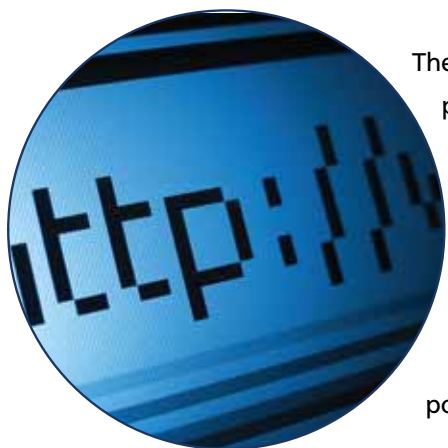
masquerade as legitimate files to gain access to your computer system. These files have the potential to allow other users access directly to your computer – exposing personal information and company secrets, or completely destroy the data on your machine.

### Bundled Software

P2P applications can often come bundled with extra software which users, by default, are encouraged to install. This software may include various forms of 'malware', 'spyware' and 'adware' which are designed to disrupt, corrupt or spy on your computer usage. These various forms of software can potentially lead to your passwords, personal files and other sensitive data being sent to an unknown third party for their use.



# P2P & the risks to children



The use of P2P networks by children leaves them vulnerable to exposure of pornographic materials including images and video. Some P2P networks play host to large-scale trafficking in pornography, even in child pornography.

The Sydney Morning Herald reported recently that children using LimeWire to search for their favourite music artist had been provided with links to pornographic images. Searches for music by such artists as Britney Spears and Christina Aguilera, and TV shows like The Wiggles or Hi 5 had returned links to pornographic images and websites exploiting children.

(Sydney Morning Herald, 20 August 2008)



## Protecting yourself at home and at school

Find out more about protecting yourself against illegal file-sharing and copyright infringement.

### school

- Check that your school has in place 'acceptable use' policies that provide students with guidelines for appropriate online behaviour
- The guidelines should highlight unacceptable behaviour such as illegal file-sharing and alert students to the dangers of doing so. These guidelines should be announced at every opportunity, by teachers and wherever possible promoted on school websites and computers
- Check that your school provides students with links to visible antipiracy campaigns and websites such as: [www.afact.com.au](http://www.afact.com.au) & [www.ipawareness.com.au](http://www.ipawareness.com.au) and promote legitimate ways of enjoying movies and television shows.

### home

- Discuss the seriousness of copyright infringement and the risks involved in participating in P2P file-sharing with your partner and children
- Be wary of movies and TV shows that appear to be available for free online. These may often be pirated copies, distributed on the internet. This is especially true of movies that have yet to show, or are currently showing in cinemas, or of television shows that have not yet been broadcast on cable or free-to-air television, and
- There are many legitimate online services which provide movie and TV shows for download.

# P2P caseSTUDIES

## ARMY MEDICAL CENTRE RECORDS BREACHED

In June 2008, an investigation was launched into the possible compromise of about 1,000 patient records at Walter Reed Army Medical Center via peer-to-peer (P2P) networking applications. The names, Social Security numbers and birth dates of the patients were among the personally identifiable information in a computer file that was shared without authorisation.

{<http://cyberinsecure.com/patients-personal-data-compromised-in-walter-reed-army-medical-center/> (3 June 2008)}

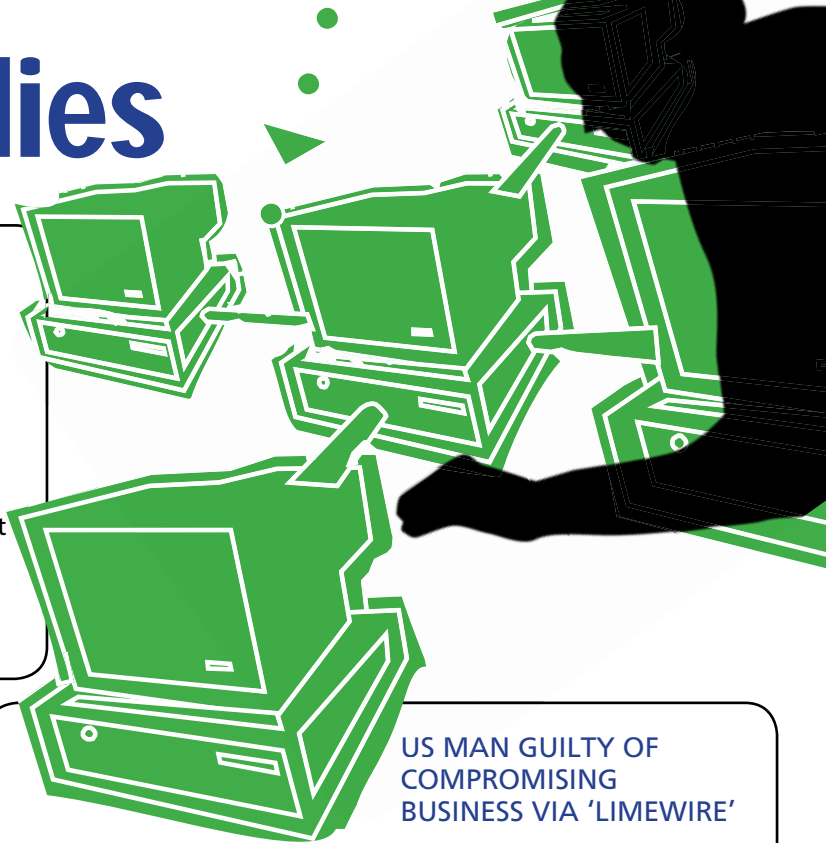
## OBAMA'S HELICOPTER SPECS AT IRANIAN IP ADDRESS

On 1 March 2009, a company that monitors P2P file-sharing networks discovered a potentially serious security breach involving President Barack Obama's helicopter. A US security company that specialises in P2P technology reportedly found engineering and communications information about Marine One at an IP address in Tehran, Iran. The company was able to trace the file back to its original source. What appeared to be a defence contractor had a file-sharing program on one of their systems that also contained highly sensitive blueprints for Marine One. It is believed that someone from the company most likely downloaded a file-sharing program, typically used to exchange music and movies, not realising the accompanying hazards. "When downloading one of these file-sharing programs, you are effectively allowing others around the world to access your hard drive," said Bob Boback, CEO of Tiversa, a leading internet security company.

{<http://www.msnbc.msn.com/id/29447088> (1 March 2009)}

**57% of Australian internet traffic is due to P2P file exchanges.**

(iPoque study 2007)



## US MAN GUILTY OF COMPROMISING BUSINESS VIA 'LIMEWIRE'

In August 2008, a 19-year-old man from Wyoming in the US, plead guilty in federal court to charges alleging that he compromised 5 to 15,000 computers by modifying the file-sharing program LimeWire, thereby obtaining the personal data of thousands of victims. He agreed to pay more than \$73,000 in restitution.

{<http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=17125> (29 August 2008)}

## P2P SECURITY BREACHES AT ABN AMRO

In September 2007, Citi's ABN Amro Mortgage Group reported that the personal information, including Social Security numbers, of more than 5,000 customers was leaked when one of its business analysts in Florida, or a member of her family, signed up to use the P2P file sharing service LimeWire on a home computer which contained the mortgage group's personal information.

{<http://www.scmagazineus.com/ABN-Amro-suffers-p2p-data-breach/article/35828/> (27 September 2007)}

## 17,000 SOCIAL SECURITY NUMBERS OF PFIZER EMPLOYEES EXPOSED

In June 2007, over 17,000 social security numbers of current and former Pfizer employees were exposed by a laptop owned by Pfizer and used by an employee. The employee's spouse used a P2P file sharing program and inadvertently shared documents containing the personal information.

{<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024491> (12 June 2008)}

# cont. case studies

## CRIMINAL USED 'LIMEWIRE' AND 'SOULSEEK' TO PILLAGE HARD DRIVES

In September 2007, a man was arrested following his use of P2P file-sharing software to steal personal information from numerous innocent victims. According to police, he used the stolen information to create false bank accounts and credit cards and then purchased thousands of dollars worth of goods. He used LimeWire and Soulseek P2P networks to carry out the thefts and investigators identified 82 victims of his activity. He was charged with mail fraud, accessing a protected computer without authorisation and two charges of aggravated identity theft. If convicted, the man faces up to 29 years in prison.

{[http://www.the-register.co.uk/2008/06/28/nugache\\_creator\\_plea\\_agreement/](http://www.the-register.co.uk/2008/06/28/nugache_creator_plea_agreement/) (28 June 2008)}

## APPLE'S iWork 09 SOFTWARE INFECTED WITH TROJAN HORSE ON BITTORRENT

In January 2009, security firms found a new Trojan horse in pirated copies of Apple's iWork 09 software, which could allow an attacker to take control of the infected computer. Security alerts rated the particular Trojan horse as "serious". When the software is newly installed, the Trojan is also installed as a start-up item, and then connects to a remote server over the Internet and could download additional components to the infected computer.

{<http://cyberinsecure.com/mac-os-x-malware-found-in-pirated-apple-iwork-09/> (22 January 2009)}

## JAPANESE DEFENCE AGENCY DOCUMENTS LEAKED

In March 2006, an employee accidentally exposed confidential documents of the Japanese Defence Agency while illegally sharing infringing materials stored on a computer set up for work purposes. Confidential information relating to training with the US Defence forces in 2005 was subsequently leaked over the file trading network.

{<http://lists.jammed.com/ISN/2006/06/0058.html> (13 June 2006)}

## TAIWANESE FILESHARING WEBSITE FOXY INDICTED ON COPYRIGHT CHARGES

The Taiwanese P2P file-sharing website Foxy was found to be illegal at a court hearing on 16 April 2009. Foxy lends itself easily to the leakage of personal information. Once installed, Foxy allows the user to search all kinds of data within seconds. However, the default file-sharing settings of Foxy means the user is sharing their entire hard disk with other users at the same time. This is equivalent to divulging personal information to the public. Previous police records have shown that, in a number of cases involving the leakage of corporate internal documents, the cause can be traced to the installation of the Foxy software. In addition, because Foxy does not have a built-in file verification mechanism, it soon becomes a breeding ground for the spread of malicious programs.

{<http://www.taipetimes.com/News/taiwan/archives/2009/04/17/2003441277> (16 April 2009)}

more info