video websites

- what's illegal
- what's at risk
- how to stay safe

WHAT IS ILLEGAL STREAMING?

Illegal streaming sites are video websites which allow the user to view movie and TV content without legitimate authorisation from the content creator.

Some unauthorised illegal streaming sites host the content themselves while others, often referred to as "linking" or "leeching" sites, link users to content stored on large file hosting websites. Unfortunately, a large number of these sites exist for the sole purpose of exploiting copyrighted material for profit, without the permission of the copyright holder.

WHAT ARE THE RISKS?

Drive-by downloads/Malvertising

Websites that focus on the distribution of copyrighted content often rely on less reputable advertising networks to make money. These networks may be susceptible to 'drive-by-downloads'.

'Drive-by-downloads' occur when hackers embed malicious code into advertisements placed on advertising networks. Once the website visitor is displayed the affected advertisement their computer is inadvertently compromised, and risks being the target of phishing attacks (spear-phishing), bank fraud and identity theft.

Advertising /Surveys

As illegal streaming sites begin to generate large volumes of traffic, they often rely on donations and advertising to pay for the cost of maintaining the site and to generate a healthy income for the site operators.

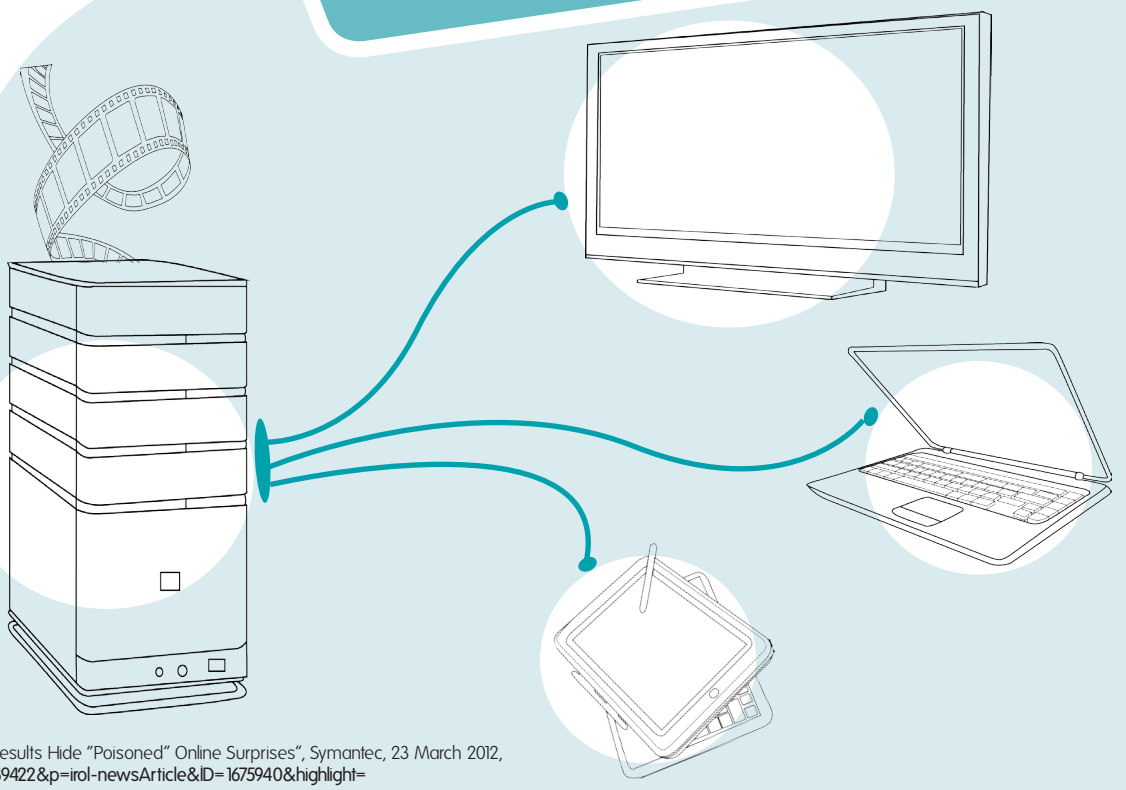
One type of advertising model which is often encountered on these sites requires the user to complete a survey, culminating in providing your mobile phone number in order to unlock the page.

This may result in you unknowingly subscribing to a Premium Rate SMS service which then charges for every SMS the company sends to your phone.

Case study -'Hunger Games'

When the film 'Hunger Games' was released in March 2012, anti-virus and security company Symantec issued a security advisory warning that cybercriminals were looking to capitalise on movie lovers curiosity by 'poisoning' links related to the film.

Symantec's press release noted that "Hunger Games free download", "Hunger Games torrent", and "Hunger Games Suzanne Collins" were returning 'poisoned' links which upon visiting, could instantly infect your computer with viruses, key logging software and other unauthorised software which has the potential to cause havoc to your smartphones, tablets and computers.



1: "MEDIA ADVISORY: "Hunger Games" Search Results Hide "Poisoned" Online Surprises", Symantec, 23 March 2012, http://investor.symantec.com/phoenix.zhtml?c=89422&p=irol-newsArticle&ID=1675940&highlight=

video websites

■ what's illegal ■ what's at risk ■ how to stay safe

Case study - McAfee (2010)

In 2010, McAfee published a report: "The true cost of free entertainment".

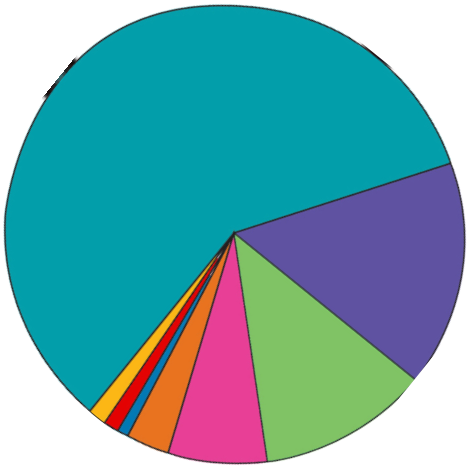
Throughout their analysis of known sites, McAfee found 12% of all sites distributing unauthorised movie and TV content were also actively distributing malware to users who downloaded content.

McAfee also found that 7% of these identified sites were associated with known cybercrime organisations. Even searching for free movies, Tv shows and other media was risky. Adding 'free' to your search in some cases, increased the risk of inadvertently downloading malware three-fold. McAfee concluded their analysis with the following statement:

"The takeaway for the consumer who is tempted to get something for free instead of purchasing it is this: long gone are the days when risks were easy to identify.

With the massive advances in cybercrime, illegal content becomes one more platform designed to attract and exploit consumers with sophisticated technology, leaving users unaware of the risks to which they have been exposed".[3]

RISKS FROM ILLEGAL SITES[2]



- 59% pornography
- 16% unknown security risks from changing content
- 12% malware
- 7% Sites registered to criminal organisations that are known to distribute malware and exploits
- 3% sites that are used for other illegal activites i.e selling credit cards, botnet access, instructions on how to conduct illegal activity etc.
- 1% Browser exploits
- 1% spam
- 1% spyware/adware/keyloggers

LINKING SITES vs CYBERLOCKERS

Many websites involved in the illegal distribution of copyrighted material can be divided into two classes, "Linking" websites and "Cyberlocker" websites.

Linking websites generally collect and index links to files on cyberlockers that contain copies of movies, TV shows and music. Users simply click on a link to begin downloading or streaming illegal content to their computers. Cyberlockers often:

- monetise their business model through ad revenues and subscriptions;
- provide incentives and rewards to users uploading 'popular content';
- remove files which have not been downloaded for a period of time;
- restrict download speed until you become a paying member.

Case study - Barracuda Labs (2012)

In 2012, Barracuda Labs conducted research into maliciousness of the Internet's top ranked domains. The most popular site found to be serving 'drive-by-download' exploits was a leeching site.

The researchers determined that on a single day in February, 745,402 users were served malicious content – potentially exposing them to fraud and identity theft.

Barracuda Labs determined that 97% of the sites that served visitors malicious content were at least one year old; and 50% were at least 5 years old. This means attackers are in many cases using well established sites for the drive-by-download attacks.[4]

2&3: Paul Greve, "Digital Music and Movie Report", McAfee 2010, http://www.mcafee.com/us/resources/reports/rp-digital-music-movies-report.pdf
4: "Maliciousness in Top-ranked Alexa Domains", Barracuda Labs, 28 March 2012, www.barracudalabs.com/wordpress/index.php/2012/03/28/maliciousness-in-top-ranked-alexa-domains/

peer to peer filesharing

- what's illegal
- what's at risk
- how to stay safe

WHAT IS P2P?

Filesharing is a method of distributing electronically stored information such as movies, TV shows or music. One of the most common filesharing 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, 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 creator and/or the copyright owner.

WHAT ARE THE DANGERS?

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

P2P Application Security

Many P2P applications can share files back onto the network to increase the amount of files on the network available to its users. This data is often set to come from your "Documents" folder where your personal information may also be stored. You may be sharing everything on your hard drive including personal files.[3]

Viruses, Worms and Trojans

Viruses, Worms and Trojans can be collectively referred to as 'malware'. These small programs are often distributed with files shared on P2P networks and masquerade as legitimate files to gain access to your computer system. These files have the potential to allow other users access directly to your home or work computer-exposing personal information and/or company information, and can completely destroy the data on your machine.

Bundled Software

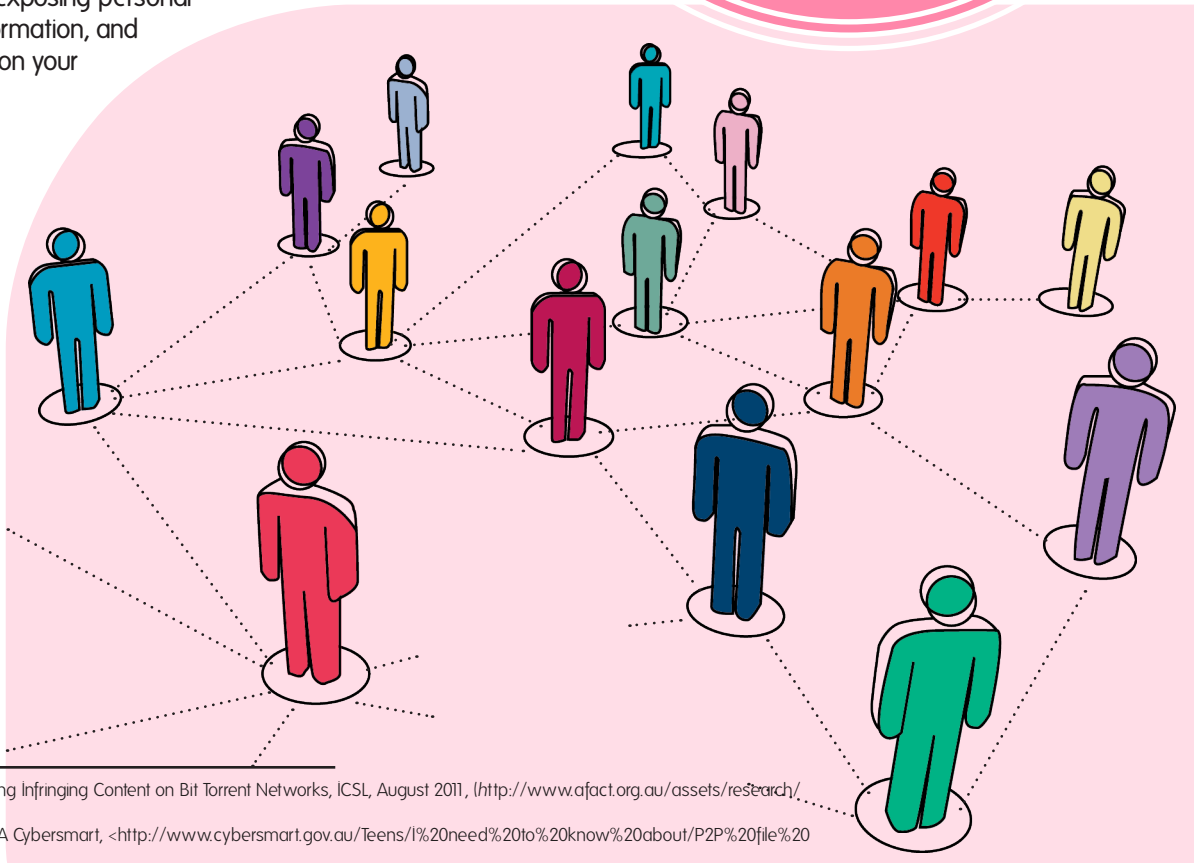
P2P applications can often come bundled with extra software which users, by default, are encouraged to install.

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.

50% of popular torrents appear to be faked files, either malware or incorrect files.[5]

97.2% of the most popular "real" torrents (i.e. not faked files) are copyright infringing.[6]



5&6: Watters, P. & Layton R., "Determining Infringing Content on Bit Torrent Networks, ICSL, August 2011, (http://www.afact.org.au/assets/research/BitTorrent_Report_2011.pdf)

7: "Cybersmart - P2P file sharing", ACMA Cybersmart, <http://www.cybersmart.gov.au/Teens/I%20need%20to%20know%20about/P2P%20file%20sharing.aspx

protecting you & your family

- what's illegal
- what's at risk
- how to stay safe

INFRINGING WEBSITES & RISKS TO CHILDREN

When children access websites expressly designed to share copyright material it leaves them vulnerable to exposure of pornographic materials including images and video. Nearly all such websites are ad-supported. Many rely on advertising pornographic websites which contain uncensored, hard-core pornographic images.

One of the most commonly searched terms on a major P2P tracker site was for child pornography material. Searches for these terms were as common as searches for the movie, 'Harry Potter".[7]

PROTECTING THEM AT HOME

- Discuss the risks involved in participating in P2P file-sharing with your children.
- Make your children aware that many files on P2P networks may be infected with viruses.[8]
- Be wary of movies and TV shows that appear to be available for free online as they may be illegal copies. For a guide on how to identify illegal DVDs and Blu-rays, please visit *afact.org.au/guide*
- There are many ways to access legal movie and TV content online. For a full list of legal providers, please visit *afact.org.au/legaloptions*

Sites most likely to carry viruses and malware are pirating or illegal file share websites.[9]

1.5 million people fall victim to some form of cybercrime daily, which cost $US110 billion annually.[10]

PROTECTING THEM AT 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.
- Check that your school provides students with links to campaigns and websites like *ipawareness.com.au* which promote legitimate ways of accessing & enjoying movies and television shows online.

NZFACT

www.nz.co.nz

7: "Searches for child porn as popular as Harry Potter: study", ABC Ballarat, 2 February 2011, http://www.abc.net.au/local/stories/2011/02/02/3128119.htm
8: "Cybersmart - P2P file sharing", ACMA Cybersmart, http://www.cybersmart.gov.au/Teens/I%20need%20to%20know%20about/P2P%20file%20sharing.aspx
9&10: "Consumer Cybercrime costs New Zealand $469.9 milion", Scoop Business 13.09.12 (http://www.scoop.co.nz/stories/BU1209/S00471/consumer-cybercrime-costs-new-zealand-4629-million.htm)