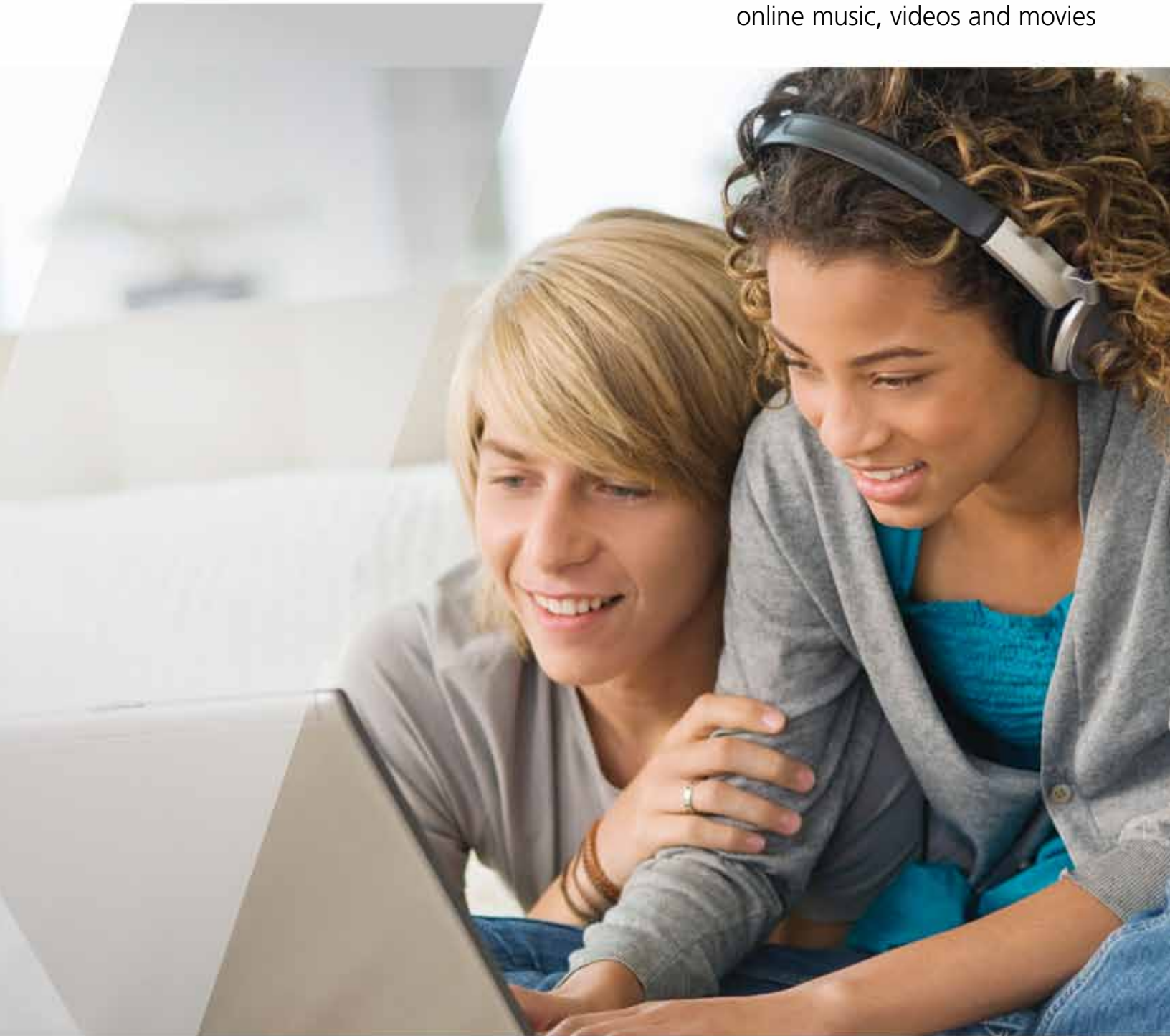


Music and Movies: Entertainment Versus Online Risk

Avoiding the risks associated with
online music, videos and movies





Introduction

Hungry for entertainment, today's consumers are increasingly turning to online media such as digital movies, music, television, radio and videos. In fact, more than 178 million U.S. Internet users watched online video in July 2010, up from 158 million a year ago.¹ While adults may click on streaming video to stay abreast of world news, teens search for posters from their favorite movie or the ringtone of the latest Lady Gaga hit. Online media gives it all to us, quickly and easily, but at a price. Accessing online entertainment without taking the necessary precautions may potentially expose consumers to numerous threats to their computers and identity.

While serious online risks exist, you can still enjoy the Internet for entertainment and information. Just arm yourself by knowing what to look for and how to protect yourself and your computer.

Social media has changed how we access entertainment and information. Cybercrooks take advantage of our fascination and immediate need for breaking news or the latest gossip to get us to click on spam emails or "must-see" videos as a means of distributing their malware and other threats. Popular social media sites such as YouTube, that had 143.2 million unique viewers in July 2010², are highly attractive to cybercriminals looking to target a mass, unsuspecting audience.

Here's a summary of the key findings from our McAfee® Labs™ research on online entertainment:

- **"Free" can be costly:** Adding the word "free" to a search for music ringtones results in a three-fold increase in the riskiness of the sites returned by major search engines in English. Translating "free" to the appropriate local language word had similar results in other native search engines.

¹ ComScore, Inc. July 2010 U.S. Online Video Rankings - http://www.comscore.com/Press_Events/Press_Releases/2010/8/comScore_Releases_July_2010_U.S._Online_Video_Rankings

² Ibid

- **“MP3s” add risk:** Searching for “MP3s” adds risk to music search results and searching for “free MP3s” makes music search results even riskier. Even when a consumer indicates that they want to pay for the MP3 in their search, results still send them to pirated content.
- **“Fans” attract dangerous URLs:** McAfee has discovered thousands of malicious and highly suspicious URLs associated with fan clubs or comments made on fan pages, even if the comments are made via social avenues such as Facebook, MySpace, YouTube and Twitter.
- **Bad ads run rampant:** Malicious advertising—where an online ad is used to distribute malware or redirect the user’s browser without their knowledge—is a common means of infection, even on well-established sites. For instance, on June 1, 2010, McAfee identified “malvertising” on perezhilton.com that redirected users to a site that delivered malware.
- **Illegal content sites often fool consumers:** Sites that are set up to distribute illegal content are difficult for consumers to detect and often distribute malware and expose users to other risks. These sites are so sophisticated that the criminal associations behind the sites can often only be found by tracking the ownership of the domains, and the relationships and tools that were used to develop those sites. Not something the average consumer can, or will, do.



Digital Movie Risks

Focusing on movies, our research revealed that these types of threats revolve around high web traffic and consumer interest. Whether it's screensavers or the latest in-demand movie, cybercriminals are attracted to these sites because they draw the most consumer interest.

Streaming media: radio, television and live video feeds

Consumers are drawn to videos because they are a fast and convenient method to view up-to-date content. World events such as the earthquake in Haiti, sporting events like the Fédération Internationale de Football Association (FIFA) World Cup or hot topics tend to generate a lot of traffic on video sites.

On the downside, the sheer demand for this type of real-time content also makes it very appealing to cybercriminals looking for a large audience to tap into. For example, in April 2010, McAfee identified websites hosted in Russia and Brazil that were advertising images and videos for the FIFA 2010 World Cup. But instead of leading visitors to World Cup content, they actually advertised rogue anti-virus programs, phished for the consumer's personal or financial information, or attempted to install malware on the user's computer.

In general, when you look online for entertainment content and information if you don't know where the content is coming from, the legitimacy of the site you are on and don't have the necessary computer security software and settings in place, you are exposing yourself to risk.

"Free" movies, screensavers and posters

How safe is it to search online for movie-related information, such as ratings, reviews and theaters? Surprisingly safe! However, that risk changes significantly when you search for "free" movies or "free screensavers" related to movies. In addition, movie posters and photos often hold unwanted surprises—such as malware.

McAfee first became aware of movie-related threats in 2009 when the highly anticipated *New Moon* trailer debuted at the MTV Music Awards. The next day, McAfee researchers noted the sudden appearance of various malware-infected *New Moon* poster JPG and GIF files in places across the Internet, such as fan forums and wiki pages. Since that time, this trend has continued for high profile, much-anticipated movies.

Movie fan sites

McAfee Labs also found risk on various movie fan sites. A movie fan, who may have little knowledge of security, visits a site to find information about their favorite celebrity. Unbeknown to the fan, the site could be infected and compromised by scammers hoping to take advantage of the fans.

And many times the attacks aren't even that sophisticated. Anyone can post a link to a malicious website or post a picture that is embedded with malware. Historically, these minor (low-traffic) sites are the easiest and most successful at infecting users. In fact, it is fairly common to find multiple fan sites built by cybercriminals with the express purpose of attempting to corral traffic to sell ads or infect users.

These minor sites owned by well-meaning movie fans are less likely to notice a security breach on their website and therefore will not take the immediate and necessary action to clean their site. McAfee has discovered a number of such sites that still retain traces of attacks that occurred several months prior.

It is fairly common to find multiple fan sites built by cybercriminals with the express purpose of attempting to corral traffic to sell ads or infect users.

Movies

Movies that are not yet widely available are known to be extremely popular search targets by cybercriminals who anticipate that a large number of people will be searching for these films online.

Consumers are wading into dangerous waters when they search for movies that are only in local theaters, not available globally or when they search for movies that are not yet available in theaters at all, such as the latest Harry Potter film.

Cybercrooks lay their traps by advertising for these high-demand movies. Once the consumer clicks on their site, the crooks give consumers fake anti-virus security software scams, dangerous tools (that are supposedly designed to help the user download and view the film or show), or drive-by exploits/downloads. (A “drive-by” attack occurs on the user’s computer when a download is performed without the user’s express authorization—no action required by the consumer, so he or she is not even aware that it has occurred.)

Governments and various industry associations have publicized the fact that pirating content violates the law, but people still continue to seek out “free.” Beyond the legal considerations, consumers need to understand the risks they bring to themselves and their computers by accessing these sites. Most notably, even if a site looks legitimate, it may not be.

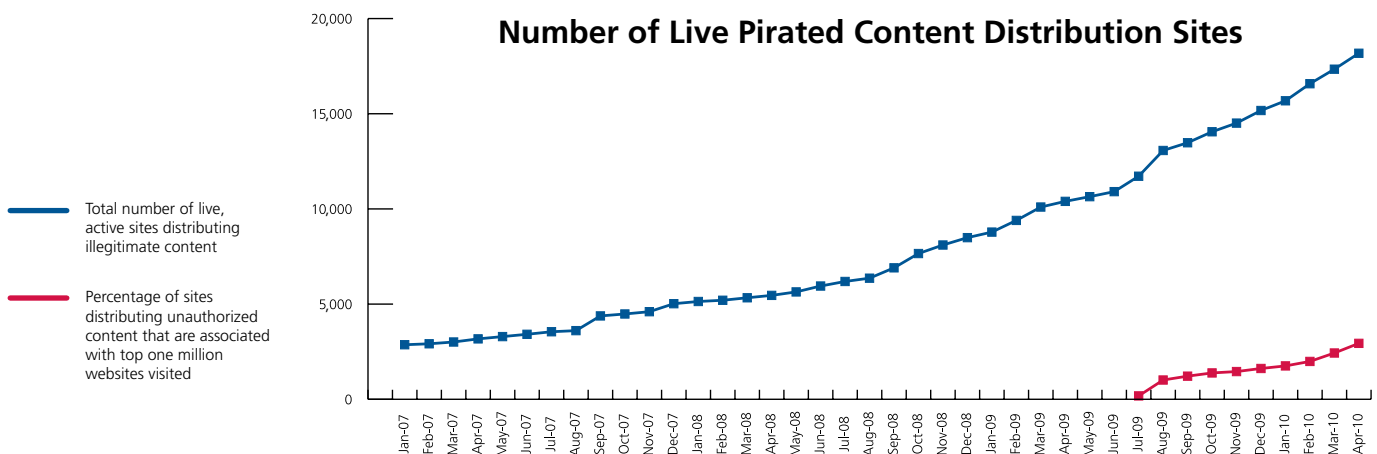
Consumers should exercise caution and ensure they have up-to-date security software that can block and remove viruses, spyware and adware from their computer.

Television

After debuting in the United States, the *Lost* television series finale was widely watched around the world with restrictions in some countries, such as Germany. But that didn’t stop some global *Lost* fans from watching the finale. They found a way to bypass these restrictions—with anonymization services. Anonymization services allow a user to be anonymous, hence masking or faking the location from which they were viewing the television show.

While anonymization services are convenient, consumers should be aware that these services cost money to maintain. Sites that distribute illegal content need to sell advertising to pay for bandwidth and storage needs and they aren’t necessarily choosy about where the money comes from. In light of this, users should be wary of providing information to these sites or downloading any tools that they offer. For example, McAfee research found a user can encounter significant “spammy advertising” once he or she registers with one of these sites.

We are seeing a growing number of websites designed solely for the purpose of attracting users and directing them to illegitimate sites. The chart below represents servers that host websites that send users to illegitimate content. The blue line details the total number of live, active sites distributing this content. The red line indicates what percentages of the sites that are distributing unauthorized content are associated with the top one million websites visited (according to Alexa).



The popularity of pirated content sites is increasing.

Sites that distribute unauthorized content are not only numerous, they can also be highly deceptive. It can be very difficult for the average consumer to determine whether these are legitimate services. That's because on these sites, users can rank movies, set up RSS feeds and even find links to legitimate websites, such as IMDb.com (The Internet Movie Database). All of these features make them more convincing to users. That's why having security software and safe-search tools installed and up-to-date are essential for the average consumer that can't detect these very deceptive sites.

Malvertising

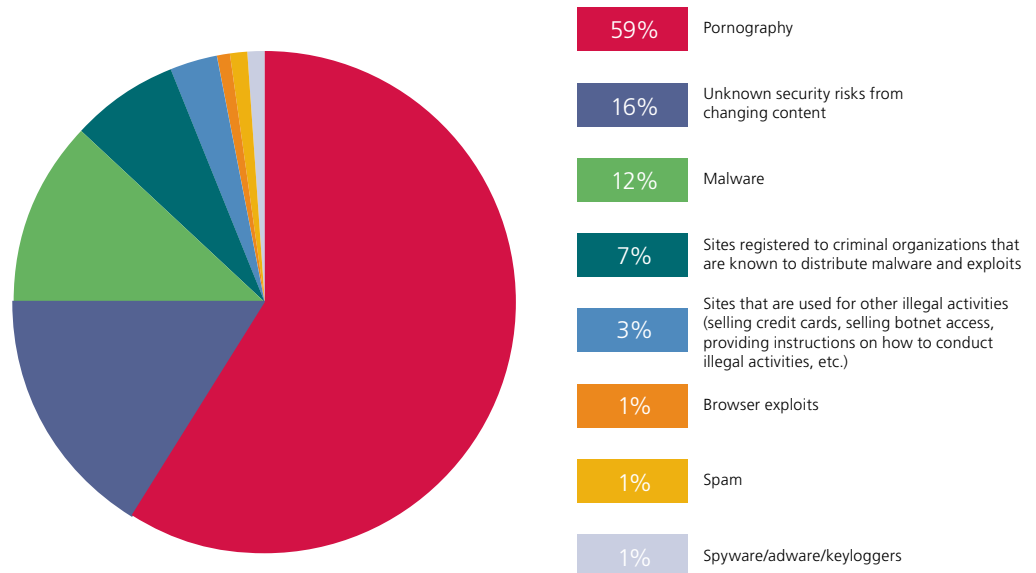
Online advertising on digital media sites is an especially effective way to get consumers to click on a dangerous link. These links may lead to a virus, a fake anti-virus website or to a browser exploit which will redirect or alter your computers settings, redirect URLs, or distribute content without your knowledge. All this is done because cybercrooks can tailor their ads to the site's audience, making them appear legitimate and appealing.

The chart on below illustrates the risks that consumers face when making the decision to use sites that advertise unauthorized or free content. Visitors may be exposed to pornography, identity theft, information theft, malware distribution and more.

Keep in mind that 7% of the websites distributing unauthorized content have associations with known cybercrime organizations. The sites often look very professional and attempt to lure the user with the idea of a "trial period" or even some nominal fee that is much less than what may ultimately be charged. Once the user submits their information, the cybercrooks have access to it and can use it for malicious purposes.

Again, consumers should remember that "free" is very often the lure used by cybercrooks and the average consumer cannot identify the illegitimacy of a claim or website. With the massive advances in cybercrime, illegal content becomes yet another platform designed to attract and exploit consumers with sophisticated technology, leaving the user unaware of the risks to which they have been exposed.

Risks From Sites That Advertise Unauthorized Content



This chart provides the details on risks associated with accessing sites that distribute unauthorized content.



Online advertising on digital media sites is an especially effective way to get consumers to click on a dangerous link.

Digital Music Dangers

There are many aspects of digital music—from lyric sites and fan pages to streaming radio and MP3 download sites—giving cybercriminals a multitude of avenues to trick unsuspecting consumers. While certain platforms, such as Apple’s iTunes store, have helped to make it easy for users to buy reputable and legitimate content, once again we found that strong demand for free content; interaction and entertainment introduced numerous risks.

MP3 downloads

Between 2009 and 2010, McAfee noted a 40% increase in the websites that are delivering infected MP3 files or seem to be built with the sole purposes of conducting some type of cybercrime (identity theft, financial fraud, malware infection, for example) on individuals looking for MP3 media files online.

Links and tweets

Cybercrooks often post malicious links in blogs and forums and drive traffic by tweeting these URLs to fans. Users click freely, and it is only after they’ve clicked on a link that they can view the content, giving cybercrooks the opportunity to spread malware without the user’s knowledge.

When McAfee conducted a search for “Lady Gaga” in May 2010, the search results turned up a link to a Lady Gaga website and fan forum. But when we clicked the link, we saw advertising leading to adult-oriented content as well as links to a “telephone video service.” The video service directed consumers to a web address where they could meet “hot, sexy, singles.” Imagine what vulnerable teens and tweens could be exposed to if they performed this search and continued clicking!

YouTube and music downloads

YouTube is a website that has greatly impacted the music industry. Any band can record their performance and post it on YouTube to be discovered, build a fan base, or just share their video with others. Malware authors are also aware of the popularity of YouTube—and they have taken full advantage of it.

In June 2010, our researchers discovered more than 700,000 web pages designed to look identical to YouTube, except that they were created to spread malware. They hooked consumers with the promise of a “must-see video” associated with the British Petroleum oil spill, the National Basketball Association (NBA) Playoffs, Harry Potter movies, and other popular topics. The fake pages even contained a YouTube logo. But when users attempted to play the videos, they were prompted to download and install a program. Clicking “OK” caused their browsers to be redirected through several other sites before landing on a final malware distribution site.

Social media makes it quick and easy for us to share information with friends and as it grows in use and popularity, this only makes it easier to spread those threats.

Music-related searches

It's not who you are that makes you dangerous; it's your ranking. That's what McAfee found when researching which music artists are the most risky search terms. Artists with top ranking on the local hit lists—whether it's the *Billboard* Top 40 in the U.S. or Australia's *ARIA* Top 50 list—were consistently riskier for fans to search for.

Here are key music-related search findings where "risk" refers to users being exposed to any of the following: adware, spyware, fake anti-virus software, malware or pornography.

- **Rank brings risk:** Searching for a popular artist and his/her current ranked hit brings up more risk than just searching for the artist.
- **Lyrics versus ringtones:** Searching for "lyrics" for a particular artist is twice as risky, on average, as searching for "ringtones" for the same artists within the first five pages of search results. However, if a user continues beyond the first five pages, then "ringtones" overall is a riskier term.
- **"Free" proves to be costly, again:** Adding the word "free" to ringtones results in a three-fold increase in the riskiness of the sites returned by the major search engines.
- **Safer to pay:** Add the word "buy" to "ringtones" and search results immediately become safer than searching for ringtones by themselves.
- **Screensavers won't save you:** Searching for the artist plus "screensaver" yielded an additional 50% increase in risk over the risk associated with "ringtones."
- **"MP3" dangers:** Searching for "MP3s" is even more risky than leaving "MP3" out of the search terms.





Summary

Cybercrime is big business and online media is one of cybercriminals' biggest moneymakers. Demand for digital media—whether it's music, videos, television, or other streaming content—is at an all time high and cybercrooks are looking to exploit its popularity in every way that they can.

As online media expands and devices change, we expect the threats to adapt and become subtler, but we don't expect them to go away. Simply searching for online media may seem safer, but the truth is cybercriminals use many different ways to distribute threats. The threats have evolved past high-level search and are more prevalent than ever.

The only way for users to protect themselves is to stay aware of the risks associated with digital media, be on the lookout for potential new dangers and use comprehensive security software.

Here are some important tips for staying safe while enjoying digital media:

- Avoid searching for "free" content. Instead, stick to legitimate, paid sites to get your music and movies
- Don't click on links in banner ads on music, movie and download sites that aren't well established.
- To safeguard from the latest threats, install comprehensive security software, such as McAfee Total Protection™ that is continuously updated and prevents, blocks and removes potential threats.
- Use common sense—don't click on links posted in forums or on fan pages, and do seek out well-established, legitimate media sites.
- Use a safe search plug-in, such as McAfee SiteAdvisor® software, to warn you of potentially risky sites in your search results.
- Realize that the more in-demand a topic, a movie, or an artist is, the higher the risk you face when searching for them.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse and shop the Web more securely. Backed by unrivaled McAfee Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee secures your digital world.

<http://www.mcafee.com>



McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
1.866.622.3911
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

McAfee, the McAfee logo, McAfee Labs, McAfee Total Protection, and SiteAdvisor are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2010 McAfee, Inc. 13201rpt_dig-music-movies_0810