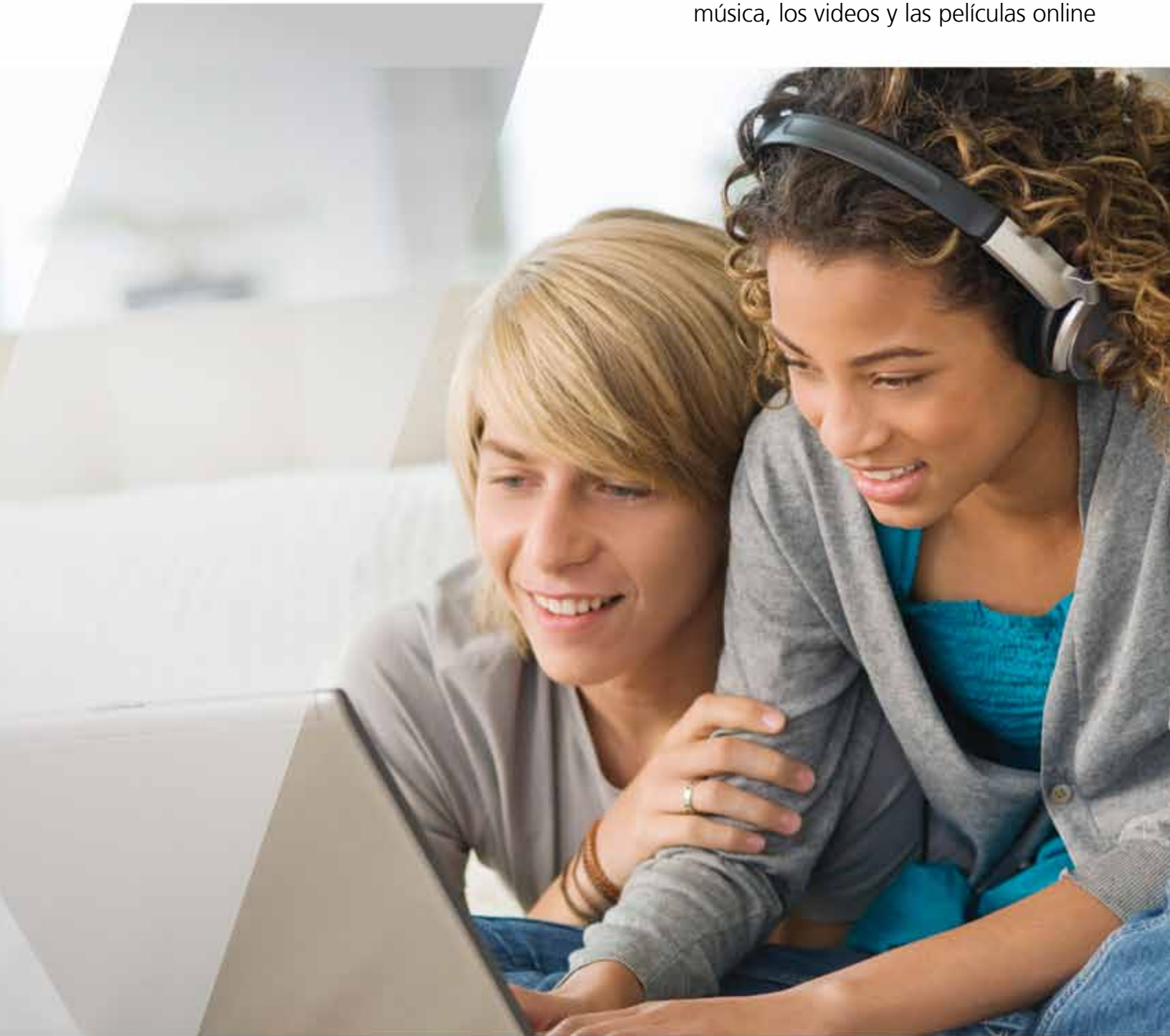


# Música y películas: Entretenimiento en comparación con el riesgo online

Cómo evitar los riesgos asociados con la  
música, los videos y las películas online





## Introducción

Los consumidores de hoy, hambrientos de entretenimiento, se inclinan cada vez más a los medios online, como películas, música, televisión, radio y videos digitales. De hecho, más de 178 millones de usuarios de Internet en los EE. UU. miraron videos online en julio de 2010, un aumento en comparación con los 158 millones del año anterior.<sup>1</sup> Si bien los adultos pueden ingresar a videos de comunicación audiovisual para mantenerse al tanto de las noticias mundiales, los adolescentes buscan afiches de sus películas favoritas o tonos de llamada (“ringtones”) del último éxito de Lady Gaga. Los medios online nos ofrecen todo de manera rápida y fácil, pero con un costo. Acceder al entretenimiento online sin tomar las precauciones necesarias podría exponer a los consumidores a numerosas amenazas para su computadora y para su identidad.

Si bien existen riesgos online graves, de todos modos puede disfrutar de Internet para obtener entretenimiento e información. Sólo prepárese y sepa qué buscar y cómo protegerse y proteger a su computadora.

Los medios sociales han cambiado el modo en que accedemos al entretenimiento y a la información. Los ciberdelincuentes (en inglés, Cybercrooks ) se aprovechan de nuestra fascinación y nuestra necesidad inmediata de noticias de último minuto o de los chismes más recientes para lograr que hagamos clic en mensajes de spam o en videos “que no podemos dejar de ver” y así distribuyen su malware y demás amenazas. Los sitios de medios sociales más populares, como YouTube, que tuvo 143.2 millones de espectadores únicos en julio de 2010<sup>2</sup>, son muy atractivos para los ciberdelincuentes que buscan como objetivo a una audiencia masiva que no sospeche de la amenaza.

Éste es un resumen de los hallazgos clave de la investigación de los laboratorios McAfee® Labs™ sobre el entretenimiento online:

- **Lo “gratis” puede salir muy caro:** Agregar la palabra “free” (gratis) a una búsqueda de tonos de llamada musicales triplica el riesgo de los sitios devueltos por los motores de búsqueda principales en inglés. Traducir “free” (gratis) al idioma local apropiado tuvo resultados similares en otros motores de búsqueda nativos.

<sup>1</sup> ComScore, Inc. Julio de 2010 Calificaciones de videos en línea de los EE. UU. - [http://www.comscore.com/Press\\_Events/Press\\_Releases/2010/8/comScore\\_Releases\\_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)

<sup>2</sup> De la misma fuente

- **Los “MP3” suman riesgos:** Buscar “MP3” suma riesgos a la búsqueda de resultados de música, y buscar “MP3 gratuitos” hace que los resultados sean aún más riesgosos. Incluso si el consumidor indica que desea pagar por el MP3 en su búsqueda, los resultados pueden enviarlo a contenido pirateado.
- **“Fanáticos” atrae URL peligrosas:** McAfee ha descubierto miles de URL maliciosas y muy sospechosas asociadas con clubes o comentarios realizados en páginas de fanáticos, incluso si los comentarios se realizan mediante sitios sociales como Facebook, MySpace, YouTube y Twitter.
- **Los anuncios malos proliferan:** La publicidad maliciosa (en la que un anuncio online se utiliza para distribuir malware o para redirigir el navegador del usuario sin que él lo sepa) es un medio común de infección, incluso en sitios de buena reputación. Por ejemplo, el 1 de junio de 2010, McAfee identificó “malvertising” en perezhilton.com que redirigía a los usuarios a un sitio que transmitía malware.
- **Los sitios con contenido ilegal a menudo engañan a los consumidores:** Es difícil que los consumidores detecten sitios establecidos para distribuir contenido ilegal, los cuales a menudo distribuyen malware y exponen a los consumidores a otros riesgos. Estos sitios son tan sofisticados que se pueden encontrar asociaciones criminales detrás de ellos si se rastrea la propiedad de los dominios y relaciones, y las herramientas que se utilizaron para desarrollarlos. Y eso no es algo que el consumidor promedio pueda o quiera hacer.



## Los riesgos de las películas digitales

En relación con las películas, nuestra investigación demostró que estos tipos de amenazas se centran en el intenso tráfico web y los intereses de los consumidores. Ya sean protectores de pantalla o la última película más pedida, los ciberdelincuentes se ven atraídos por estos sitios porque concentran el mayor interés de los consumidores.

### **Medios de comunicación audiovisual: radio, televisión y alimentaciones de video en tiempo real**

Los consumidores se ven atraídos por los videos porque son un método rápido y conveniente para visualizar contenidos actualizados. Los hechos mundiales como el terremoto en Haití, los eventos deportivos, como la Copa Mundial de la Federación Internacional de Asociaciones de Fútbol (FIFA) o los temas candentes suelen generar mucho tráfico en los sitios de videos.

La desventaja es que la demanda de este tipo de contenido en tiempo real también es muy seductora para los ciberdelincuentes que buscan una gran audiencia a la cual interceptar. Por ejemplo, en abril de 2010, McAfee identificó sitios web hospedados en Rusia y Brasil que promocionaban imágenes y videos publicitarios de la Copa Mundial de la FIFA 2010. Pero en lugar de mostrar a los visitantes el contenido de la Copa Mundial, en realidad, publicitaban programas falsos de antivirus, obtenían de manera fraudulenta (en inglés, phished) información personal o financiera del consumidor o intentaban instalar malware en la computadora del usuario.

Por lo general, cuando usted busca entretenimiento e información online sin saber de dónde proviene el contenido ni la legitimidad del sitio en el que se encuentra, y si además no cuenta con un software de seguridad con la configuración adecuada, se expone a un riesgo.

### **Películas, protectores de pantalla y afiches “gratuitos”**

¿Cuán seguro es realizar una búsqueda online de información relacionada con películas, como calificaciones, críticas y salas de cine?  
¡Sorprendentemente seguro! Sin embargo, ese riesgo cambia significativamente cuando busca películas “gratuitas” o “protectores de pantalla gratuitos” relacionados con películas. Asimismo los afiches y las fotografías de películas generalmente contienen sorpresas no deseadas, como el malware.

McAfee identificó por primera vez las amenazas relacionadas con películas en 2009, cuando el muy esperado avance de *Luna Nueva* debutó en los premios MTV Music Awards. Al día siguiente, los investigadores de McAfee notaron la aparición repentina de varios afiches de *Luna Nueva* con formato .JPG y archivos .GIF infectados con malware en sitios de Internet, como foros de fanáticos y páginas de Wiki. Desde ese entonces, esta tendencia ha continuado para las películas de alto perfil y muy esperadas.

### **Sitios de fanáticos de películas**

McAfee Labs además encontró más riesgos en varios sitios de fanáticos de películas. Un fanático de películas, que puede tener pocos conocimientos sobre seguridad, visita un sitio para encontrar información sobre su celebridad favorita. Sin que el fanático lo sepa, el sitio podría estar infectado y comprometido por estafadores que buscan aprovecharse de los fanáticos.

Y muchas veces los ataques ni siquiera son muy sofisticados. Cualquier persona puede publicar un enlace a un sitio web malicioso o una fotografía con malware. Históricamente, estos sitios menores (de poco tráfico) son los que más fácil y con mayor éxito infectan a los usuarios. De hecho, es muy común encontrar múltiples sitios de fanáticos creados por ciberdelincuentes con el propósito expreso de congregar tráfico para vender anuncios o infectar usuarios.

Estos sitios menores, que son propiedad de fanáticos de películas bien intencionados, tienen menos probabilidades de notar el incumplimiento de seguridad en el sitio y, por lo tanto, no toman inmediatamente las medidas necesarias para limpiarlo. McAfee ha descubierto varios sitios de este tipo que todavía conservan rastros de ataques que ocurrieron varios meses antes.

Es muy común encontrar múltiples sitios de fanáticos creados por ciberdelincuentes con el propósito expreso de congregar tráfico para vender anuncios o infectar usuarios.

## Películas

Se sabe que las películas que no se encuentran todavía disponibles para el público general son blancos de búsqueda muy populares para los ciberdelincuentes, que prevén que una gran cantidad de personas las estarán buscando online.

Los consumidores caminan por terreno peligroso al buscar películas que están solamente en los cines locales, que no están disponibles mundialmente o que todavía no están en cines, como la última película de Harry Potter.

Los ciberdelincuentes tienden a trampa con publicidades de estas películas de gran demanda. Una vez que el consumidor hace clic en el sitio, los estafadores les dan a los consumidores software de seguridad antivirus falsos, herramientas peligrosas (que supuestamente están diseñadas para ayudar a los usuarios a descargar y ver películas o programas) o descargas/ataques ocultos a vulnerabilidades. (Un ataque "inadvertido" sucede en la computadora del usuario cuando se realiza una descarga sin su autorización explícita: sin necesidad de que el consumidor realice acción alguna, por lo que el consumidor no se da cuenta de que ha ocurrido eso).

Los gobiernos y varias asociaciones industriales han declarado que la piratería de contenido viola la ley, pero la gente continúa buscando contenidos "gratuitos". Más allá de las consideraciones legales, los consumidores deben comprender los riesgos que corren ellos y sus computadoras al acceder a estos sitios. Sobre todo, deben saber que aunque un sitio parezca legítimo, puede no serlo.

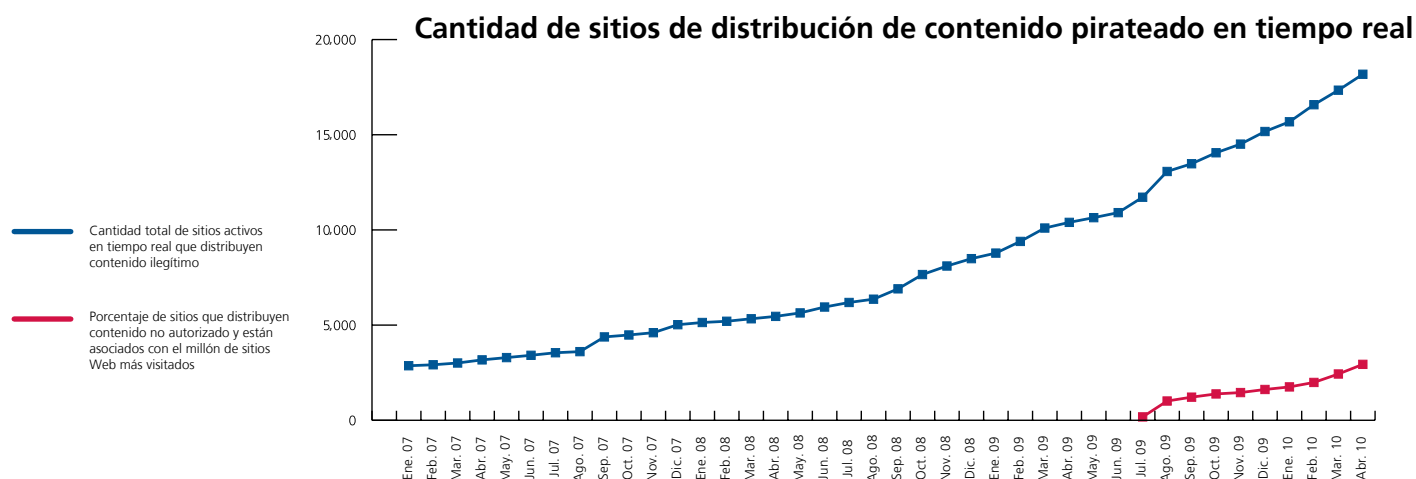
Los consumidores deben ser precavidos y asegurarse de contar con software de seguridad actualizado que pueda bloquear y eliminar virus, spyware y de su computadora.

## Televisión

Luego de su estreno en los Estados Unidos, el episodio final de la serie de televisión *Lost* fue muy visto en todo el mundo, con restricciones en algunos países, como Alemania. Pero eso no detuvo a algunos fanáticos que vieron el episodio final en todo el mundo. Encontraron el modo de evitar las restricciones, mediante servicios de anonimato. Los servicios de anonimato le permiten al usuario ser anónimo y, por lo tanto, enmascaran o falsifican la ubicación desde la cual está viendo el programa de televisión.

Si bien los servicios de anonimato son convenientes, los consumidores deberían saber que estos servicios se mantienen con dinero. Los sitios que distribuyen contenido ilegal necesitan vender publicidad para pagar las necesidades de ancho de banda y almacenamiento, y no son necesariamente exigentes en cuanto al origen del dinero. Es por esto que los usuarios deben ser cautelosos al brindarles información a estos sitios o al descargar las herramientas que ofrecen. Por ejemplo, la investigación de McAfee descubrió que un usuario puede encontrar mucha "publicidad spam" una vez que se registra en uno de estos sitios.

Vemos cada vez más sitios web diseñados exclusivamente con el propósito de atraer usuarios y dirigirlos a sitios ilegítimos. El cuadro a continuación representa los servidores que hospedan sitios web que envían a los usuarios hacia contenido ilegítimo. La línea azul indica la cantidad total de sitios activos en tiempo real que distribuyen este contenido. La línea roja indica qué porcentaje de sitios que distribuyen contenido no autorizado están asociados con el millón de sitios Web más visitados (según Alexa).



La popularidad de los sitios web de contenido pirateado aumenta.

Los sitios que distribuyen contenido no autorizado no sólo son muchos sino que también pueden ser muy engañosos. Puede ser muy difícil para el consumidor promedio determinar si son servicios legítimos o no. Eso se debe a que en dichos sitios los usuarios pueden calificar películas, establecer alimentadores de RSS e incluso encontrar enlaces a sitios web legítimos, como IMDb.com (The Internet Movie Database). Todas estas funciones los hacen más convincentes para los usuarios. Por ello es fundamental que el consumidor promedio, que no puede detectar estos sitios tan engañosos, tenga instalados y actualizados un software de seguridad y herramientas de búsqueda seguras.

### Malvertising

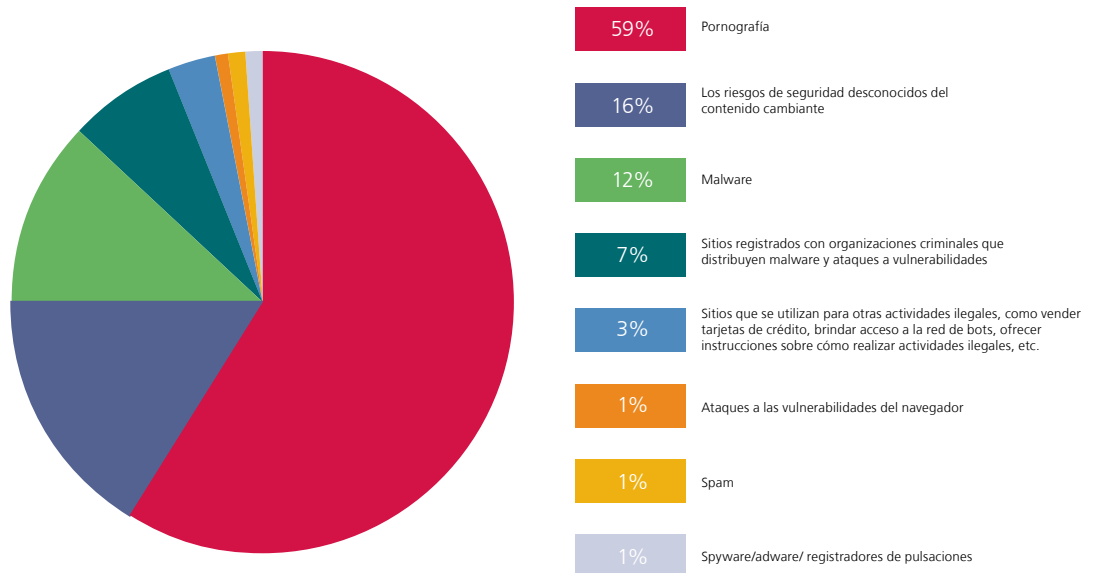
La publicidad online en sitios de medios digitales es una manera especialmente efectiva para lograr que los consumidores hagan clic en un enlace peligroso. Esos enlaces pueden conducir a virus, a un sitio web falso de un antivirus o a un ataque a la vulnerabilidad del navegador que redirigirá o alterará las configuraciones de su computadora, redirigirá las URL o distribuirá contenidos sin que usted lo sepa. Todo esto sucede porque los ciberdelincuentes pueden adaptar sus publicidades según cuál sea la audiencia del sitio, y así parecen legítimas y atractivas.

El cuadro que se presenta a continuación ilustra los riesgos que los consumidores enfrentan al tomar la decisión de utilizar sitios que publican contenido no autorizado o gratuito. Los visitantes pueden verse expuestos a pornografía, robo de identidad, robo de información, distribución de malware y más.

Recuerde que el 7% de los sitios web que distribuyen contenido no autorizado tienen asociaciones con organizaciones de ciberdelitos conocidas. A menudo, lo sitios parecen muy profesionales e intentan atraer al usuario con la idea de un "período de prueba" o incluso una tarifa nominal mucho menor de lo que se podría cobrar en última instancia. Una vez que el usuario envía la información, los ciberdelincuentes acceden a ella y la pueden utilizar con fines maliciosos.

Una vez más, los consumidores deben recordar que "gratuito" es generalmente el atractivo que usan los ciberdelincuentes y que el consumidor promedio no puede identificar la ilegitimidad de una afirmación o de un sitio web. Con los enormes avances en los ciberdelitos, el contenido ilegal se convierte en una plataforma más, diseñada para atraer y aprovecharse de los consumidores con tecnología sofisticada, mientras que el usuario ignora los riesgos a los que ha sido expuesto.

## Riesgos de sitios que publicitan contenido no autorizado



Este cuadro detalla los riesgos asociados con el acceso a sitios que distribuyen contenido no autorizado.



La publicidad online en sitios de medios digitales es una manera especialmente efectiva para lograr que los consumidores hagan clic en un enlace peligroso.

## Peligros de la música digital

Muchos de los aspectos de la música digital, desde los sitios de letras de canciones y páginas de fanáticos hasta los sitios de descarga de radio y MP3, les brindan a los ciberdelincuentes una gran cantidad de maneras de engañar a los consumidores desprevenidos. Si bien algunas plataformas, como iTunes store de Apple Inc., han ayudado a facilitarles a los usuarios la compra de contenido legítimo y de confianza, nuevamente descubrimos que esa fuerte demanda de contenido gratuito, de interacción y de entretenimiento ha introducido varios riesgos.

### Descargas de MP3

Entre 2009 y 2010, McAfee notó un aumento del 40% en los sitios web que entregan archivos MP3 infectados o que parecen estar creados con el único objetivo de cometer algún tipo de ciberdelito (robo de identidad, fraude financiero, infección de malware, entre otros) contra los individuos que buscan archivos MP3 en línea.

### Enlaces y tweets

Los ciberdelincuentes a menudo publican enlaces maliciosos en blogs y foros, y manejan el tráfico enviándoles a los fanáticos estas URL a través de tweets. Los usuarios hacen clic despreocupadamente y sólo luego de haber hecho clic en un enlace, pueden ver el contenido. Eso les da a los ciberdelincuentes la oportunidad de esparcir programas perjudiciales sin el conocimiento del usuario.

Por ejemplo, McAfee realizó una búsqueda de "Lady Gaga" en mayo de 2010. Los resultados de la búsqueda mostraron un enlace a un sitio web de Lady Gaga y a un foro de fanáticos. Pero cuando hicimos clic en el enlace, vimos publicidades que conducían a contenido para adultos y a enlaces para un "servicio de video telefónico". Este servicio de video dirigía a los consumidores a una dirección web en la que podían conocer "solteras sexies y seductoras". Imagínese a lo que podían exponerse los adolescentes y preadolescentes si realizaban esta búsqueda y continuaban haciendo clic.

### YouTube y descargas de música

YouTube es un sitio web que ha impactado de manera significativa la industria de la música. Cualquier banda que quiera ser descubierta puede grabar su tema y publicarlo en YouTube, crear una base de fanáticos o simplemente compartir videos con otras personas. Los autores de malware también son conscientes de la popularidad de YouTube y se aprovechan totalmente de esa herramienta.

En junio de este año, nuestros investigadores descubrieron más de 700,000 páginas web diseñadas con el objetivo de que se vieran idénticas a YouTube, salvo por el hecho de que eran creadas para esparcir malware. Atraían a los consumidores con la promesa de un "video que debe mirar" relacionado con el derrame de petróleo británico, los juegos de National Basketball Association (NBA), películas de Harry Potter y otros temas populares. Las páginas falsificadas incluso contenían un logotipo de YouTube. Pero cuando los usuarios intentaban reproducir los videos, se les pedía que descargaran e instalaran un programa. Cuando hacían clic en "OK", se redirigía el explorador a muchos otros sitios antes de llegar, finalmente, a un sitio de distribución de malware.

Los medios sociales hacen que sea más rápido y más fácil para nosotros compartir información con nuestros amigos y, a medida que crecen en usos y en popularidad, hacen que sea más fácil esparcir amenazas.

### Búsquedas relacionadas con la música

No es usted lo que lo vuelve peligroso; es su calificación. Esto es lo que descubrió McAfee cuando investigó qué artistas musicales constituyen los términos de búsqueda más riesgosos. Los artistas mejor clasificados en las listas de éxitos locales, ya sea *Billboard* Top 40 en los Estados Unidos o ARIA Top 50 en Australia, resultaron ser mucho más riesgosos para los fanáticos.

Éstos son algunos hallazgos clave relacionados con la búsqueda de música. "Riesgo" significa que los usuarios se exponen a cualquiera de estas amenazas: adware, spyware, software de antivirus falso, malware y pornografía.

- **El ranking conlleva riesgos:** Buscar un artista popular y su éxito actual conlleva más riesgos que simplemente buscar el artista.
- **Letras en comparación con tonos de llamadas:** Buscar "letras" de canciones de un artista en particular es dos veces más riesgoso (en promedio) que buscar tonos de llamada del mismo artista, dentro de las primeras cinco páginas con resultados de la búsqueda. Sin embargo, si un usuario va más allá de las primeras cinco páginas de resultados, en general "tonos de llamada" es un término más riesgoso.

- **Una vez más, lo "gratis" puede salir muy caro:** Agregar la palabra "gratis" a los resultados de tonos de llamadas triplica el riesgo de los sitios devueltos por los principales motores de búsqueda.
- **Es más seguro pagar:** Agregue la palabra "comprar" a "tonos de llamada" y los resultados de la búsqueda inmediatamente se tornan más seguros que cuando busca "tonos de llamada" solamente.
- **Los protectores de pantalla no lo protegerán:** Buscar el artista, más "protector de pantalla" demostró tener un riesgo adicional del 50% sobre el riesgo asociado con los "tonos de llamada".
- **Los peligros de los "MP3":** Buscar "MP3" es incluso más riesgoso que quitar "MP3" de los términos de la búsqueda.





## Resumen

El ciberdelito es un gran negocio y los medios online constituyen una de las entradas de dinero más importantes de los ciberdelincuentes. La demanda de medios digitales, ya sea música, videos, televisión u otro contenido audiovisual, está en aumento constante y los ciberdelincuentes buscan aprovechar su popularidad de todas las maneras posibles.

A medida que crecen los medios online y que cambian los dispositivos, esperamos que las amenazas se adapten y sean más sutiles, pero no esperamos que desaparezcan. Buscar simplemente los medios online puede parecer más seguro, pero la realidad es que los ciberdelincuentes usan muchas formas diferentes de distribuir amenazas. Las amenazas han evolucionado, superaron la búsqueda de alto nivel y son más frecuentes que nunca.

La única manera que tienen los usuarios de protegerse consiste en conocer los riesgos asociados con los medios digitales, estar atentos a los posibles peligros nuevos y utilizar software integral de seguridad.

Aquí tiene algunos consejos importantes para mantenerse a salvo mientras disfruta de los medios digitales:

- Evite buscar contenido "gratis". En cambio, apéguese a sitios legítimos y pagos para obtener música y películas.
- No haga clic en espacios publicitarios de sitios de descarga de música y películas que no tengan una buena reputación.
- Para protegerse de las amenazas más recientes, instale un software de seguridad integral, como McAfee Total Protection™ el cual se actualiza constantemente y evita, bloquea y elimina las posibles amenazas.
- Use el sentido común: no haga clic en enlaces publicados en foros o en páginas de fanáticos. Busque sitios de medios legítimos y con una reputación sólida.
- Use un complemento de búsqueda segura, como el software McAfee SiteAdvisor® para que le advierta sobre sitios potencialmente riesgosos en los resultados de su búsqueda.
- Recuerde que cuanto mayor es la demanda de un tema, película o artista, mayor es el riesgo que enfrenta al buscarlo.

## Acerca de McAfee, Inc.

McAfee, Inc., con sede en Santa Clara, California, es la empresa dedicada a la tecnología de seguridad más importante del mundo. La empresa brinda servicios y soluciones proactivas y comprobadas que ayudan a hacer más seguros los sistemas, las redes y los dispositivos móviles en todo el mundo, y permiten a los usuarios conectarse, navegar y comprar en Internet con mayor seguridad. Respaldada por la inigualable inteligencia contra amenazas globales, McAfee Global Threat Intelligence, McAfee crea productos innovadores que ayudan a los usuarios, a las empresas, al sector público y a los proveedores de servicios y les permite cumplir con las regulaciones, proteger datos, prevenir interrupciones, identificar vulnerabilidades y controlar y mejorar continuamente la seguridad. McAfee protege su mundo digital.

<http://www.mcafee.com>



McAfee, Inc.  
2821 Mission College Boulevard  
Santa Clara, CA 95054  
1.866.622.3911  
[www.mcafee.com](http://www.mcafee.com)

La información incluida en este documento se proporciona sólo con fines educativos y para la conveniencia de los clientes de McAfee. La información incluida en este documento está sujeta a cambios sin aviso previo y se proporciona "EN ESTAS CONDICIONES", sin garantía con respecto a la exactitud o utilidad de la información de cualquier situación o circunstancia específica.

McAfee, el logotipo de McAfee, McAfee Labs, McAfee Total Protection y SiteAdvisor son marcas registradas o marcas comerciales de McAfee, Inc. o sus filiales en los Estados Unidos y en otros países. Otras marcas pueden reclamarse como propiedad de otros. Los planes, las especificaciones y las descripciones del producto en este documento han sido proporcionados sólo con fin informativo y están sujetos a cambios sin previo aviso, y se proporcionan sin ningún tipo de garantía, expresa o implícita. Copyright © 2010 McAfee, Inc  
13201rpt\_dig-music-movies\_0810