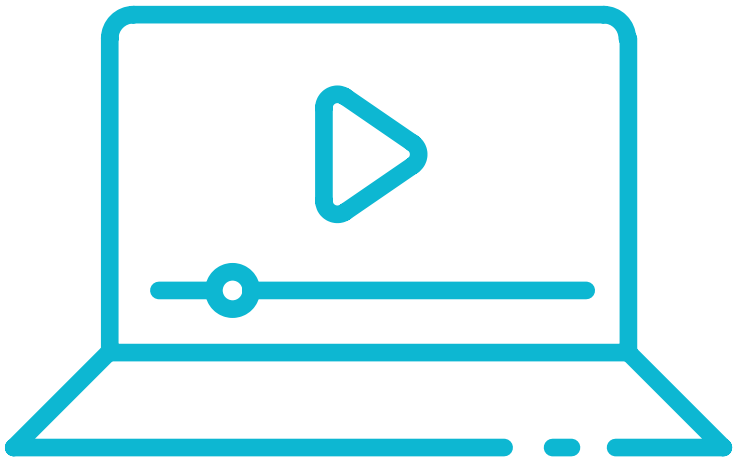
15 years ECC-Net

European Consumer Centre Network

ECC-Net, junio de 2020
en cooperación con F & M A



SAFER STREAMING

Amenazas de los servicios de vídeo bajo demanda ilegales y qué puede hacer al respecto

ÍNDICE

LA TRANSMISIÓN DE VÍDEO ESTÁ EN AUGE

La comodidad de poder ver el programa favorito cuando más convenga y en cualquier dispositivo hace que los servicios de transmisión de vídeo sean la nueva norma para los usuarios actuales.

En los últimos años, la tecnología de transmisión de vídeo ha modificado el panorama multimedia, fundamentalmente por haber combinado con éxito los mundos de Internet y de la televisión. Con esta rentabilidad, muchas empresas de transmisión consiguen invertir más que el sector del cine tradicional para producir importantes series y películas, con lo que consiguen aún más audiencia.

60%

del tráfico de descarga global en Internet es de vídeo.[2]

Un 42%

más de suscripciones a transmisión de vídeo en Europa cada año.[3]

El 89%

de los mileniales utilizan la transmisión de vídeo.[4]

Actualmente, la mayoría del ancho de banda mundial de Internet lo consume la transmisión de vídeo. Durante la crisis del coronavirus en la primavera de 2020, subió tanto que la Comisión Europea instó a los principales proveedores a que redujesen la calidad de vídeo, con el fin de garantizar la velocidad de Internet para servicios más importantes como las reuniones web de teletrabajo.[5]

Fuentes: 1 A companion to Television 2 Sandvine 3 EUROVOD 4 Forbes 5 EU commission

DOS SISTEMAS DE VÍDEO BAJO DEMANDA

El **vídeo bajo demand**a le permite ver lo que quiera, cuando quiera y, si el dispositivo móvil está conectado correctamente, también donde quiera, sin necesidad de descargar contenido, ya que lo que se ve es una transmisión de datos. Puede conectarse mediante una smart TV, ordenadores de todo tipo, smartphones, tabletas e incluso videoconsolas.

IPTV

(TELEVISIÓN POR PROTOCOLO DE INTERNET)

Las empresas de difusión que proporcionan señal por cable o satélite ahora también ofrecen TV basada en Internet. La mayoría de espectadores que reciben contenido de IPTV a través de su conexión de Internet de banda ancha disponen de descodificadores o smart TV y eligen qué ver en una guía de programas. Eventos deportivos, emisiones en directo y noticias siguen siendo la espina dorsal de los canales de televisión convencionales que están disponibles actualmente en directo o a la carta.

SERVICIOS DE OTT

(LIBRE TRANSMISIÓN)

Cuando hablamos de transmisión de vídeo, solemos referirnos a empresas OTT, localmente y en toda Europa, como Netflix, Amazon Prime o Sky/NOW TV.[1] Esos servicios pueden proporcionarse a cualquier dispositivo conectado, independientemente del proveedor de servicios de Internet o de la red de ancha banda específica. La gran variedad de series de TV y películas sirve para conseguir nuevos clientes. Las producciones nuevas, originales y exclusivas también resultan muy atractivas.

Fuentes: 1 EAO yearbook

FALSO FRENTE A ILEGAL

Las descargas ilegales de material pirateado se han reducido en los últimos años, porque los usuarios prefieren utilizar sitios web seguros, cómodos y con un precio razonable, en lugar de arriesgarse a usar fuentes que podrían hacer que descargasen archivos infectados, junto con el peligro de enfrentarse a problemas legales.[1]

Los sitios web legítimos de transmisión de vídeo se financian mediante modelos de publicidad, alquiler y suscripción. Las desviaciones ilegales de esta actividad se han convertido en una amenaza constante y están ocupando poco a poco el lugar de tipos de piratería más antiguos. Otro problema son los sitios web de estafas que simulan ofrecer suscripciones o contenido.

LOS SITIOS WEB DE ESTAFAS

Atrapan a consumidores poco avanzados con suscripciones falsas y hacen un uso indebido de sus datos personales.

LOS SITIOS WEB PIRATAS

Intentan aparentar ser legítimos para atraer a los usuarios y que vean o compren contenido robado (al tiempo que les roban información privada).

Fuentes: 1 EUIPO

SITIOS WEB DE TRANSMISIÓN FALSOS:

¡SOCORRO, ME HAN ATRAPADO!

Un truco que suelen utilizar los estafadores es presentar una página principal nada sospechosa con imágenes o avances de contenido multimedia tentador accesible gratuitamente durante un periodo de tiempo limitado.

Cuando ya se ha registrado, se da cuenta de que, después de todo, no puede acceder al contenido prometido. Como no ha pagado nada, puede que le dé la impresión de que no se han producido daños y es probable que lo deje pasar.

A los pocos días, le llegará una factura que exige el pago de varios cientos de euros por una suscripción anual e indica que la prueba gratuita se convierte automáticamente en una suscripción anual cuando se cumple el periodo de prueba de unos días.

SITIOS WEB DE TRANSMISIÓN FALSOS:

HARÁN UN USO INDEBIDO DE SUS DATOS

La mayoría de sitios web de estafas no alojan **ningún contenido en absoluto.**

Hay cientos de sitios así, con la misma plantilla, por toda Europa, probablemente a cargo de los mismos delincuentes. Pasado un tiempo, desaparecen si reciben más advertencias o si los cierran por mandato judicial, lo que hace que el dominio fraudulento resulte menos rentable. Los sitios web reaparecen al poco tiempo con nuevos nombres de dominio para comenzar una nueva ronda de estafas.

Además de vender suscripciones falsas, estos sitios web obtienen beneficios del phishing**: vender datos personales que introducen los usuarios durante el registro..**[1]

Algunos sitios web falsos llegan a enviar mensajes personales por correo electrónico o SMS tras el registro, en los que requieren más datos personales por motivos de seguridad. Todos los datos se recopilan para ponerlos a la venta, a menudo a otras organizaciones criminales.

Fuentes: 1 Europol

SITIOS WEB DE TRANSMISIÓN FALSOS:

MANIPULACIÓN DEL DISPOSITIVO

Otra fuente de ingresos para los estafadores es la publicidad. Puede aparece publicidad emergente intensa en la pantalla. A menudo, incluye contenido sospechoso, está programada para que sea difícil deshacerse de ella y si se hace clic en ella, el operador siempre obtiene beneficios. Bien al intentar eliminar la publicidad, con falsos mensajes de error **o, más habitualmente, al instalar** software de visualización **o** códecs **falsificados que permiten visionar el contenido prometido, hay veintiocho veces más probabilidades de que los usuarios infecten el dispositivo con virus y malware, como:**[1]

PUP: **programas potencialmente no deseados, software molesto e inútil que ralentiza el dispositivo.**

ADWARE: **muestra de publicidad intrusiva que no se sabe de dónde sale.**

MALWARE: **software malicioso que entrega sus datos o hace un uso indebido de los recursos del dispositivo.**

SCAREWARE: **muestra mensajes de error falsos o falsos avisos de denuncia, que le acusan de haber hecho algo ilegal y le exigen el pago de una sanción o cargos por asistencia técnica.**

RANSOMWARE: **cifrado de datos en el sistema y chantaje para que pueda recuperar el acceso.**

VIRUS Y TROYANOS: **destrucción del sistema del dispositivo o robo de datos personales, como contactos, o habilitación secreta de acceso por una puerta trasera a sus sistema.**

Fuentes: 1 IP Crime Threat Assessment 2019

SITIOS WEB ILEGALES:

VENTA DE CONTENIDO ROBADO

Los sitios web ilegales, que son distintos a los sitios web de estafas, permiten a los usuarios ver contenido, pero proporcionan material robado que está protegido por derechos de autor**, lo que les quita ingresos legítimos a los creadores del contenido y a los contribuyentes, mientras beneficia a los delincuentes informáticos organizados. Utilizar esos sitios web perjudica al público en general.**

Los usuarios también pueden encontrarse con combinaciones de sitios web piratas y falsos. Esos sitios web fingen tener una gran biblioteca y tientan a los clientes para que se suscriban mostrando transmisiones de vídeo gratuitas. El catálogo completo es un fraude en esos casos y el contenido de la prueba limitada ayuda a retrasar el momento en que las víctimas se dan cuenta y anulan los pagos.

Los sitios web ilícitos intentan tener el aspecto más legítimo posible **ante los posibles clientes. Sisu ilegalidad no es obvia, habrá más gente que utilice su servicio.**

En ocasiones, no resulta fácil identificar un sitio web ilegal inmediatamente, ya que copian las interfaces de usuario de plataformas legítimas. Se detectó que aparecía publicidad de 46 de las 100 empresas globales más importantes en algún sitio web que infringe los derechos de autor. Los delincuentes saben que la publicidad de marcas conocidas hace que su portal tenga más credibilidad.

Fuentes: 1 Europol

SITIOS WEB ILEGALES:

SIN PROTECCIÓN PARA LOS MÁS JÓVENES

A los delincuentes no les preocupa la protección de los niños frente al contenido perjudicial. Los adolescentes y los niños aún no han desarrollado límites saludables **y son especialmente vulnerables mientras** usan los dispositivos móviles**, casi siempre** demasiado**. Son impulsivos y no entienden la legitimidad del contenido. El hecho de que el 56 % de los sitios web estén solo en inglés no ayuda. Los sitios web ilegales suelen incluir contenido pornográfico o** que puede herir la sensibilidad **de otras formas, y publicitan servicios de juegos de azar o apuestas, todo lo cual es totalmente inadecuado para audiencias jóvenes. Los sitios web ilegales no impiden que los menores de edad se registren.[1]**

---

1 de cada 3

usuarios de Internet es un menor.[2]

1 de cada 2

menores de 11 a 16 años se ha encontrado con riesgos habituales de Internet.[3]

Padres y madres pueden buscar consejo en betterinternetforkids.eu

Fuentes 1 IZI study 2 UNICEF 3 LSE study

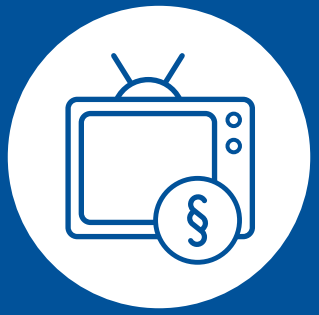
TOTALMENTE CARGADO Y CON JAILBREAK: ¿QUÉ ES ESO?

El contenido pirateado no se restringe a la tecnología OTT, sino que también supone un problema para la IPTV. Hay dispositivos de hardware ilícitos que son perjudiciales por diferentes motivos. Las denominadas cajas **Kodi** son complementos de reproductores multimedia que convierten una smart TV en un centro multimedia totalmente operativo. Se venden versiones **«totalmente cargadas»** de Kodi con funciones manipuladas para emitir transmisiones pirateadas adicionales desde fuentes de IPTV ilegales.

Los dispositivos electrónicamente inseguros **y manipulados son fuente de riesgos. Suelen ser imitaciones baratas del original, como en el caso de los** Amazon Firesticks**, importados del Lejano Oriente. Estos distribuidores a menudo son eliminados de las plataformas comerciales en línea, como** eBay**, antes de que se entreguen los pedidos.**

A los dispositivos con jailbreak **se les han deshabilitado los límites mediante un sistema operativo y** dejan de disfrutar de la cobertura de la garantía. **Si hay problemas técnicos, los fabricantes y vendedores se negarán a ofrecer una reparación o un reembolso. El intento de realizar jailbreak puede provocar un** bloqueo para el propietario **del sistema operativo, lo que haría que el dispositivo quedase inservible.**

El hardware ilícito puede contener malware **y dejar abierta una puerta trasera para que le** jaqueen **la red de la vivienda.**



Los clientes que compran dispositivos ilegales se arriesgan a perder dinero si la Europol cierra los proveedores ilegales **o si esos servicios dejan de funcionar por miedo a que se adopten medidas legales. Los agentes de aduana o las autoridades reguladoras de los mercados pueden confiscar pedidos de hardware ilícito antes de que lleguen a su casa. Si se llevan a cabo acciones policiales, quienes cargan contenido pueden tener problemas legales si se los identifica en las bases de datos de los servidores confiscados.**

Fuentes 1 SBRCentre

CARGA E INTERCAMBIO

El contenido que se puede encontrar en las plataformas de intercambio casi siempre está protegido por leyes de derechos de autor. Su **distribución** sin permiso **infringe los derechos de autor y las condiciones de uso**. Cargar contenido protegido sin permiso se considera ilegal.

Ripear **consiste en grabar las transmisiones de vídeo y guardarlas en archivos. Los sitios web que ofrecen esta posibilidad le intentarán convencer de que es legal, pero los tribunales no opinan lo mismo. Usar herramientas de descarga o grabación de la pantalla, o cargar contenido con derechos de autor son actividades que prohíben las condiciones de uso de las plataformas legales y cometer estas infracciones puede provocar la** pérdida de la cuenta de usuario.[1]

Acceda a las las preguntas frecuentes sobre derechos de autor[2] **de su país.**

Muchos usuarios de OTT comparten sus cuentas con amigos y familiares. Más del 66 por ciento de los usuarios de Netflix comparten la contraseña**, lo que da un resultado de 2,5 espectadores por cuenta. De momento, las plataformas de OTT no han tomado medidas contra este fenómeno por motivos de marketing, pero esto podría cambiar.[3]**

Fuentes: 1 IFPI 2 EUIPO 3 Global Web Index

REDES SOCIALES Y TRANSMISIONES ILEGALES

Además de las posibilidades de marketing con 3000 millones de usuarios en las redes sociales, los delincuentes explotan su característica principal: la capacidad de **compartir**. Cada vez se publican más enlaces que llevan adonde se aloja el contenido ilegal o a transmisiones ilícitas, y las transmisiones deportivas piratas alcanzan audiencias altísimas.[1]

Las series o películas completas y nuevas o las transmisiones deportivas no están disponibles legalmente en estos canales no oficiales. Los propietarios del contenido toman medidas legales contra las transmisiones ilegales en redes sociales y plataformas de intercambio de vídeo. Esto puede provocar la eliminación de cuentas de usuario si se comparte sin permiso la transmisión de vídeo. Aunque únicamente sea para uso personal.

Internet hace que sea posible usar y compartir datos y contenido a una escala sin precedentes y eso es estupendo, pero todos tienen derecho a decidir por sí mismos si, cuándo y cómo compartir su propio contenido. Tenga en cuenta que esto no cambiará con la nueva directiva sobre derechos de autor de la que es posible que haya oído hablar.[2]

Fuentes: 1 Irdeto 2 Directive EU 2019/790

COSAS QUE CONVIENE SABER

Existen numerosas ofertas legales y las descargas ilegales han disminuido desde que las ofertas han mejorado y es cada vez más fácil acceder a ellas. Además de los proveedores de OTT principales, puede visitar estos enlaces para ver otras plataformas que respetan los derechos de autor:

General: agorateka.eu

Deportes: sroc.info

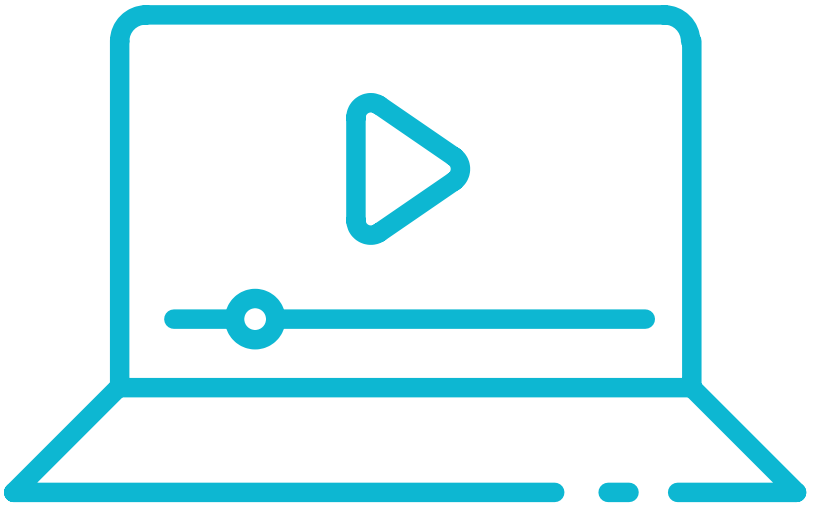
Música: pro-music.org

Las aplicaciones de transmisión de vídeo **le permiten terminar de ver una transmisión activa en otro dispositivo. Esto es muy práctico cuando se viaja y resulta imposible terminar una película de una sola vez.**

Como la directiva de portabilidad **es aplicable en todos los Estados miembros de la UE, debe poder acceder a las transmisiones de su suscripción independientemente de en qué parte de la UE esté. Ya no se aplican recargos o limitaciones por usar su servicio de transmisión de vídeo en el extranjero, mientras se encuentre en territorio de la UE.[1]**

Fuentes: 1 EU Commission

APÉNDICE



QUÉ HACER Y QUÉ NO HACER

EXAMINE EL SITIO WEB DETENIDAMENTE ANTES DE REGISTRARSE

No acceda a sitios web que tengan mala reputación.

Si busca sitios web de transmisión de vídeo y encuentra algo interesante, no se registre directamente. Dedique unos minutos más a comprobar las reseñas y las advertencias.

¿Incluyen contenido inédito?

¿La película que se anuncia aún está en los cines y ya la tienen, antes que ninguna otra plataforma de transmisión de vídeo establecida? Desconfíe.

Compare la oferta con la competencia consolidada.

¿El precio es insuperablemente más bajo que en otras plataformas? ¿Un año entero de suscripción a precio bajísimo u otras ofertas demasiado buenas para ser verdad?

COMPROBACIONES ANTES DE REGISTRARSE, N.º 2

¿Hay errores en el texto?

Los sitios web de estafas se elaboran con plantillas genéricas en varios idiomas. Las faltas de ortografía o los errores gramaticales deben hacernos sospechar.

¿Hay publicidad de apuestas, pornografía o de VPN en el sitio web, que aparecen quizá en molestos anuncios emergentes?

Las ofertas sospechosas suelen combinarse. Los sitios legales no hacen un uso excesivo de la publicidad emergente.

Busque pistas. ¿Hay pie de imprenta? ¿Hay condiciones de servicio y otra información legal?

Los sitios web de estafas no muestran información de contacto o incluyen direcciones que son falsas o son direcciones pantalla. Carecen de la información legal obligatoria o es falsa.

COMPROBACIONES ANTES DE REGISTRARSE, N.º 3

¿Se permite que los usuarios carguen contenido en el sitio?

Un indicador de su carácter ilegal es la opción de que los usuarios carguen contenido que no hayan creado ellos mismos.

¿Afirman que son legales o dan consejos sobre cómo ponerse en contacto con ellos si se produce un bloqueo?

El bloqueo por parte de los proveedores de servicios de Internet, afirmaciones vacías de legalidad y el anuncio de servidores proxy para sortear los bloqueos del sitio web son síntomas de ilegalidad.

¿Está prohibido el sitio web en los listados del buscador o aparece en listas negras de portales de advertencia?

Si un buscador ha prohibido el sitio web o un guardián de Internet advierte sobre él, infórmese bien antes de registrarse.

COMPROBACIONES ANTES DE REGISTRARSE, N.º 4

¿Hay algún botón del tipo Tramitar pedido ya? ¿El sitio web le informa sobre los costes?

Conforme a las leyes europeas, los sitios web deben mostrar claramente los costes al cliente y ofrecer una solución de botón para que los usuarios confirmen el establecimiento de un contrato comercial.

¿Hay alguna forma de contactar con la atención al cliente?

No es posible acceder a la atención al cliente, si es que se ofrece en el sitio web. Si nadie responde a su consulta, no se suscriba.

Utilice tarjeta de crédito o un servicio de pago en línea.

Esto le permitirá, en el peor de los casos, utilizar la devolución o acudir a la atención al cliente del servicio de pago. Además, los operadores obtienen una información menos personal sobre usted.

¿YA HA CAÍDO EN SUS REDES? ¿QUÉ PUEDE HACER AHORA?

No pague nada.

A menudo, las facturas de los estafadores parecen estar redactadas de forma agresiva por alguien que afirma ser un abogado o una agencia de cobro de pagos. No se deje intimidar por eso.

Informe a la autoridad a cargo de delitos informáticos.

Informe de su experiencia a la policía y al servicio de listas negras de Internet para advertir a otros.

Pida consejo a su **oficina local del CEC**[1]

Si no tiene claro si las afirmaciones son legítimas o se da cuenta de que se acaba de suscribir en un sitio web de estafas, pida consejo a su oficina local del CEC.

Fuentes: 1 ECC Net

European Consumer Centre Network

Puede encontrar más información sobre la ECC-Net aquí.

Puede encontrar más información sobre FAMA aquí.

Pie de imprenta
Fecha de publicación **junio de 2020**
Dirección/autoría del proyecto **CEC Austria**
Gráficos **Christina Zettl /** buero41a.at

Centro Europeo del Consumidor en Austria
Mariahilfer Straße 81, A-1060 Viena
www.europakonsument.at
www.facebook.com/europakonsument.at
Correo electrónico: info@europakonsument.at

Esta publicación recibió la financiación del Programa del Consumidor de la Unión Europea (2014-2020).

Co-funded by the European Union

NUESTRA MISIÓN

La red de 30 centros europeos del consumidor (CEC) permite a los consumidores conocer sus derechos y aprovechar todas las oportunidades que ofrece el Mercado Único.

CÓMO ALCANZAMOS NUESTRA MISIÓN

Los expertos legales de la ECC-Net ayudan a los consumidores a resolver problemas internacionales sin cobrarles nada y ponen a su disposición sus amplios conocimientos legales. La red ofrece una visión general única e información fiable sobre asuntos relacionados con el consumidor en el Mercado Único, que pueden utilizarse para la elaboración de políticas, en colaboración con actores clave de los panoramas europeo y nacional.

Film & Music Austria (FAMA) **ofreció asistencia para el contenido y con la traducción de textos.**

RENUNCIA DE RESPONSABILIDAD

El contenido de esta publicación representa exclusivamente los puntos de vista del autor y son responsabilidad únicamente suya. No puede considerarse que refleje los puntos de vista de la Comisión Europea o de la Agencia Ejecutiva de Consumidores, Salud y Alimentación (CHAFEA) o de cualquier otro organismo de la Unión Europea. La Comisión Europea y la Agencia no aceptan responsabilidad alguna por el uso que pueda darse a la información aquí contenida.
Responsabilidad de los enlaces: el material informativo contiene enlaces a sitios web externos de terceros. El contenido de los sitios web será responsabilidad del proveedor o del operador respectivos de los sitios web a los que dirigen los enlaces. Las ofertas legales mencionadas son ejemplos documentados de importantes empresas del mercado. Su mención no representa una aprobación de los productos o servicios que ofrece.