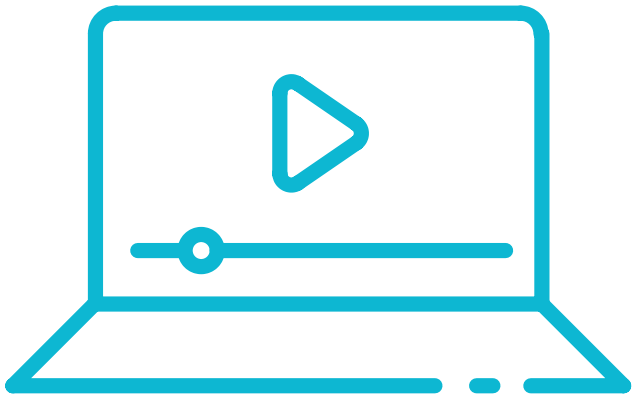
15 years ECC-Net

European Consumer Centre Network

ECC NET - Giugno 2020
in collaborazione con F & M A



SAFER STREAMING

Minacce di servizi video on demand illegali e cosa si può fare a riguardo

SOMMARIO

LO STREAMING È IN PIENA ESPANSIONE

Poter vedere il proprio programma preferito quando si vuole su qualsiasi dispositivo, fa dei servizi di streaming video il nuovo punto di riferimento dei consumatori moderni.

Negli ultimi anni la tecnologia dello streaming ha cambiato radicalmente il panorama dei mezzi di comunicazione, integrando efficacemente il mondo online a quello televisivo. Grazie a queste possibilità redditizie, molte aziende di streaming sono in grado di investire più del classico settore cinematografico per produrre serie televisive e film esclusivi, facendo crescere ancora di più il loro pubblico.[1]

60%

del traffico internet globale in downstream è video[2]

42%

in più di abbonamenti di streaming in Europa ogni anno[3]

89%

della "generazione Y" sono in streaming[4]

Oggi la maggior parte della banda larga globale di Internet viene consumata in streaming. Durante la crisi dovuta al coronavirus, nella primavera del 2020, il fenomeno ha raggiunto un tale livello che la Commissione UE ha esortato i principali provider a ridurre la qualità video per garantire la velocità di navigazione in internet per i servizi più importanti, come le riunioni web per l'home office.[5]

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

DUE SISTEMI DI SERVIZI VOD

Il *Video on Demand* consente di guardare quello che si vuole, quando si vuole, con un dispositivo mobile collegato correttamente, anche dove si vuole, senza la necessità di scaricare contenuti mentre si guardano dati in streaming. È possibile connettersi utilizzando una smart TV, computer di ogni tipo, smartphone, tablet e persino console di gioco.

"Internet protocol television" (IPTV)

Le affermate società di radiodiffusione che forniscono segnali via cavo o via satellite offrono adesso anche la TV via Internet. La maggior parte degli spettatori che riceve contenuti IPTV attraverso una connessione internet a banda larga ha configurato una top box o una smart TV e sceglie da una guida di programmi elettronica. Gli eventi sportivi, le trasmissioni in diretta e le notizie rimangono la il punto forte delle reti televisive più convenzionali, ora disponibili in diretta o su richiesta.

SERVIZI "OVER THE TOP" (OTT)

Quando si parla di streaming, di solito ci si riferisce alle aziende OTT, sia locali sia europee, come Netflix, Amazon Prime o Sky/NOW TV.[1] Tali servizi possono essere erogati a qualsiasi dispositivo collegato, indipendentemente dal fornitore di servizi Internet o dalla rete a banda larga dedicata. Ricche librerie di serie TV e film esercitano una considerevole attrattiva sui clienti. Anche produzioni nuove, originali ed esclusive sono decisamente fonte di interesse.

fonti: 1 EAO yearbook

FALSO O ILLEGALE

I download illegali di materiale pirata sono diminuiti negli ultimi anni[1], perché gli utenti preferiscono utilizzare siti sicuri, convenienti e a prezzi ragionevoli invece di rischiare con fonti che potrebbero comportare il download di file infetti, unitamente al rischio di un'azione penale da parte delle forze dell'ordine.

I siti di streaming legali sono finanziati dalla pubblicità, dal noleggio e dai modelli di abbonamento. Le deviazioni illegali di queste attività sono diventate una minaccia costante e sostituiscono sempre più spesso i vecchi tipi di pirateria. Un altro problema è rappresentato dai siti di frode che fanno solo finta di offrire abbonamenti o contenuti.

SITI DI FRODE

Ingannano consumatori inesperti tramite abbonamenti falsi per così abusare dei loro dati personali.

SITI PIRATA

Cercano di sembrare legittimi per adescare gli utenti a guardare o acquistare contenuti rubati (mentre si impadroniscono dei loro dati privati).

fonti: 1 EUIPO

SITI DI STREAMING FASULLI –

AIUTO, MI HANNO FREGATO!

Un trucco comune dei truffatori è quello di presentare un'insospettabile prima pagina con foto o trailer di contenuti multimediali allettanti e accessibili per un breve periodo di prova gratuita.

Una volta registrato, l'utente scopre, in realtà, di non poter accedere ai contenuti promessi. Dal momento che non è stato pagato nulla, viene da pensare che non si sia subito alcun danno e si tende a ignorare la vicenda.

Qualche giorno dopo si riceverà una fattura con la richiesta di diverse centinaia di euro per un abbonamento annuale, in cui si dichiara che la prova gratuita si è trasformata automaticamente in un abbonamento annuale al termine del periodo di prova di qualche giorno.

SITI DI STREAMING FASULLI –

SI VERIFICHERÀ UN ABUSO DEI DATI PERSONALI DELL'UTENTE

La maggior parte dei siti web di frode in streaming non ospita **alcun contenuto.**

Centinaia di siti di questo tipo seguono lo stesso modello e sono creati in tutta Europa, spesso dagli stessi criminali. Dopo un certo periodo di tempo scompaiono se ricevono diverse segnalazioni o se vengono bloccati dalle forze dell'ordine e questo rende il dominio fraudolento meno redditizio. I siti ricompaiono poco dopo con nuovi nomi di dominio, iniziando un nuovo ciclo di frodi.

Oltre a vendere abbonamenti falsi, questi siti traggono profitto dal phishing**: vendono i dati personali inseriti dagli utenti durante la registrazione .**[1]

Alcuni siti falsi inviano anche messaggi personali via e-mail o SMS dopo la registrazione, sostenendo di richiedere ulteriori dati personali per motivi di sicurezza.
Tutti i dati vengono raccolti per essere venduti, spesso ad altre **imprese** criminali**.**

fonti: 1 Europol

SITI DI STREAMING FASULLI –

MANIPOLAZIONE DEL DISPOSITIVO

Un'altra fonte di reddito per i truffatori è la pubblicità. È possibile che appaiano sullo schermo annunci pop-up aggressivi. Spesso mostrano contenuti dubbi, sono programmati in modo da essere difficili da eliminare, e il continuo farci clic sopra per cancellarli reca profitto all'operatore. Tentando di rimuovere gli annunci, i messaggi di errore fasulli **o, più comunemente, installando** un software o un codec di visualizzazione **fasullo per consentire la visione dei contenuti che ci si aspettano, gli utenti hanno una probabilità ventotto volte maggiore di infettare il proprio dispositivo con virus e malware come ad esempio:**[1]

PUP **- programmi potenzialmente indesiderati, software fastidiosi e inutili che rallentano il dispositivo**

ADWARE **- che mostra pubblicità invadente proveniente dal nulla**

MALWARE **- software dannoso che diffonde i dati personali o abusa delle risorse del dispositivo dell'utente**

SCAREWARE **- che mostra falsi messaggi di errore o false notifiche di procedimenti penali da parte delle autorità, contenenti l'accusa di aver commesso qualcosa di illegale e la richiesta del pagamento di sanzioni o di spese per l'assistenza tecnica**

RANSOMWARE **- che crittografa i dati del sistema di un soggetto e lo ricatta perché possa riottenerne l'accesso**

VIRUS E TROJAN **- che distruggono il sistema del dispositivo o rubano dati personali come i contatti o abilitano segretamente l'accesso alla backdoor del sistema**

fonti: 1 IP Crime Threat Assessment 2019

SITI ILLEGALI –

VENDITA DI CONTENUTI RUBATI

A differenza dei siti falsi, i siti illegali consentono agli utenti di guardare i contenuti, ma forniscono materiale rubato protetto da copyright**, che sottrae agli artefici dei contenuti creativi e ai contribuenti le dovute entrate, alimentando al contempo la scena del crimine informatico associato. L'utilizzo di tali siti danneggia il pubblico in generale!**

Gli utenti possono anche imbattersi in una combinazione di siti pirata e falsi. Tali siti fingono di avere una libreria ben nutrita e convincono i clienti all'abbonamento mostrando alcuni contenuti streaming gratuiti. Il catalogo completo è una frode in questi casi e il limitato contenuto della prova contribuisce a ritardare la presa di coscienza delle vittime e impedirne il pagamento anticipato.

I siti web illeciti cercano di apparire il più possibile legittimi **ai potenziali clienti. Quandola natura illegale non è evidente, sempre più persone utilizzano il loro servizio.**

A volte non è facile identificare subito un sito illegale in quanto vengono copiate le interfacce utente delle piattaforme legittime. Delle prime 100 aziende globali, ne sono state individuate 46 che hanno almeno una pubblicità di un brand su un sito web che viola il diritto d'autore.[1] I criminali sanno che le pubblicità di brand noti rendono il loro portale più plausibile.

fonti: 1 Europol

SITI ILLEGALI –

NESSUNA PROTEZIONE NEI CONFRONTI DEI PIÙ GIOVANI

I criminali non si preoccupano di proteggere i minori dai contenuti dannosi. Adolescenti e minori non hanno sviluppato adeguate barriere **e sono particolarmente vulnerabili quando** usano i loro **dispositivi** mobili in modo eccessivo.[1] **Sono impulsivi e non comprendono la legittimità dei contenuti. Il fatto che il 56% di tutti i siti web sia solo in inglese non migliora la situazione. I siti illegali spesso presentano contenuti pornografici o di altro tipo** nocivo**, oppure pubblicizzano servizi di gioco d'azzardo o di scommesse, tutto assolutamente inadatto a un pubblico minorile. I siti illegali non impediscono la registrazione dei minori.**

1su3

utenti internet è un minore[2]

1su2

ragazzi di 11-16 anni hanno sperimentato i comuni rischi di internet[3]

I genitori possono vedere betterinternetforkids.eu **per trovare qualche suggerimento**

fonti 1 IZI study 2 UNICEF 3 LSE study

“FULLY LOADED” E “JAILBROKEN” – DI COSA SI TRATTA?

I contenuti piratati non si limitano alla tecnologia OTT, ma sono un problema anche nell’IPTV. Esistono dispositivi hardware illeciti che sono dannosi per diversi motivi. Le cosiddette **Kodi** box sono degli accessori per lettori multimediali che permettono di aggiornare una smart TV a un vero e proprio media center. Le versioni **“fully loaded”** delle Kodi vengono vendute con funzionalità manipolate per trasmettere ulteriori contenuti piratati da fonti illegali IPTV.

I pericoli derivano da dispositivi manipolati elettronicamente non sicuri.[1] **Spesso si tratta di imitazioni a basso costo dell’originale, come nel caso di Amazon Firesticks, importati dall’Estremo Oriente. Tali rivenditori sono spesso anche rimossi dalle piattaforme di commercio online come eBay prima della consegna degli ordini effettuati.**

Nei dispositivi jailbroken **vengono disabilitate le restrizioni da un sistema operativo e** non sono più coperti da garanzia**. In caso di problemi tecnici, i produttori e i venditori si rifiuteranno di ripararli o rimborsarli. Il tentativo di jailbreaking può** bloccare il proprietario fuori **dal sistema operativo, rendendo inutile un dispositivo.**

L’hardware illecito può contenere malware **e lasciare una backdoor aperta per** hackerare **la rete domestica.**

I clienti che acquistano dispositivi illegali rischiano di perdere denaro ogni volta che l’Europol blocca i fornitori illegali **o se tali servizi si interrompono per paura delle forze dell’ordine. I funzionari doganali o le autorità di regolamentazione del mercato possono confiscare gli ordini di hardware illeciti durante il trasporto. In caso di intervento della polizia, gli uploader possono affrontare problemi legali se vengono identificati nei database dei server confiscati.**

fonti 1 SBRCentre

CARICAMENTO E CONDIVISIONE

I contenuti presenti sulle piattaforme di condivisione sono per lo più protetti dalle leggi sul diritto d'autore. La **distribuzione** senza autorizzazione costituisce una **violazione dei diritti d'autore e dei termini d'uso**. Il caricamento di contenuti protetti senza autorizzazione è considerato illegale.

Il ripping si verifica quando la trasmissione sullo schermo viene registrata e salvata in un file. I siti che offrono questa possibilità ingannano l'utente con pretese di legalità, ma i Tribunali non sono d'accordo.[1] L'uso di strumenti di download o di registrazione dei contenuti trasmessi sullo schermo o il caricamento di contenuti protetti da copyright è proibito nei termini di utilizzo delle piattaforme legali e la violazione può portare alla perdita dell'account utente.

Accedi al copyright che riguarda[2] **il tuo Paese.**

Molti utenti OTT condividono i loro account con amici e familiari. Oltre il 66% degli utenti di Netflix condivide le password**, con il risultato di 2,5 spettatori per account.[3] Per ora, gli OTT non hanno intrapreso azioni contro questo fenomeno per motivi di marketing, ma questo potrebbe cambiare.**

fonti: 1 IFPI 2 EUIPO 3 Global Web Index

SOCIAL MEDIA E STREAMING ILLEGALE

Oltre alle possibilità di marketing con 3 miliardi di utenti sui social media, i criminali ne stanno sfruttando la caratteristica principale: la capacità di **condividere**. Sempre più spesso vengono pubblicati link a siti ove vengono ospitati contenuti illegali o streaming illeciti e, soprattutto, le trasmissioni sportive pirata in diretta raggiungono un pubblico enorme.[1]

I film appena usciti, le nuove serie o le trasmissioni sportive non sono disponibili legalmente su questi canali non ufficiali. I proprietari dei contenuti intervengono contro lo streaming illegale sui social media e sulle piattaforme di condivisione video. Ciò può portare alla cancellazione degli account utente se lo streaming è stato condiviso senza autorizzazione. Anche se è solo per uso personale.

Internet rende possibile l'utilizzo e la condivisione di dati e contenuti su una scala senza precedenti ed è fantastico, ma ognuno ha il diritto di decidere autonomamente se, quando e come condividere i propri contenuti. Questa situazione non cambierà con la nuova Direttiva sul diritto d'autore di cui forse avete sentito parlare.[2]

fonti: 1 Irdeto 2 Directive EU 2019/790

UTILE DA SAPERE

Esistono molte offerte legali e i download illegali sono diminuiti dal momento che le offerte sono sempre migliori e più facilmente disponibili ogni giorno. Oltre ai principali provider OTT, è possibile controllare questi link per individuare le piattaforme che rispettano i diritti d'autore:

generico: agorateka.eu

sport: sroc.info

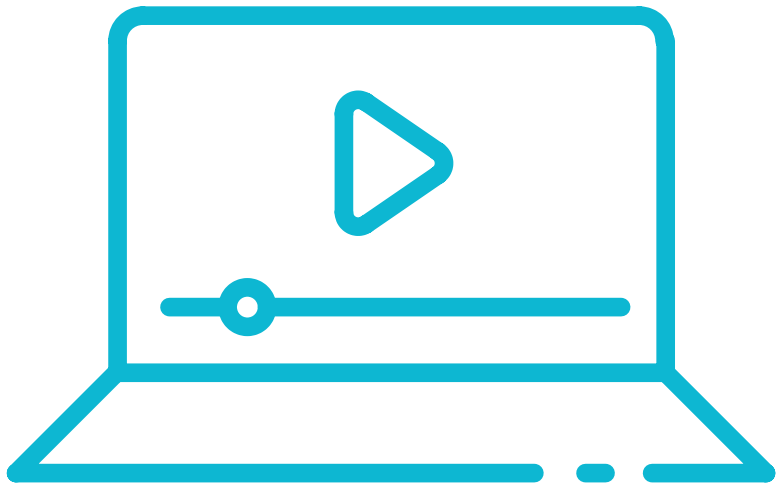
musica: pro-music.org

Le app per streaming **consentono di finire di vedere una trasmissione in esecuzione su un dispositivo diverso. Questo è utile quando si viaggia e non si riesce a finire di guardare un film in una sola volta.**

Poiché la direttiva sulla portabilità[1] si applica a tutti gli Stati membri dell'UE, gli abbonamenti di streaming devono essere forniti all'utente indipendentemente dalla sua ubicazione all'interno dell'UE. Non è più previsto un supplemento o un divieto di utilizzare il servizio di streaming all'estero mentre l'utente si trova sul territorio dell'UE.

fonti: 1 EU Commission

PRIEDAS



COSE DA FARE E DA NON FARE

DATE UN'OCCHIATA APPROFONDITA PRIMA DI ISCRIVERVI!

Non entrare in siti con una cattiva reputazione!

Se si cercano siti di streaming e si trova qualcosa di interessante, non è necessario iscriversi subito. Meglio aspettare un altro minuto per controllare le recensioni e le segnalazioni.

Presentano contenuti inediti?

Il film pubblicizzato è ancora nelle sale cinematografiche e ce l'hanno già prima di qualsiasi altra piattaforma di streaming affermata? È una cosa che puzza!

Confrontate l'offerta con i concorrenti affermati!

È decisamente più economico di altre piattaforme? Un abbonamento per un anno intero a un prezzo davvero basso o altre offerte troppo vantaggiose per essere vere?

CONTROLLI PRIMA DI ISCRIVERSI N. 2

Ci sono errori di testo?

I siti di frode sono realizzati con modelli generici in diverse lingue. Errori ortografici o grammaticali indicano un'origine dubbia.

Sono presenti pubblicità di scommesse, pubblicità pornografiche o di reti virtuali private (VPN) sul sito, magari mostrate in fastidiosi popup?

Le offerte dubbie compaiono spesso combinate. I siti legali non abusano di un'eccessiva pubblicità tramite pop-up.

Cercate gli indizi! C'è un marchio? Sono offerti termini di servizio e altre informazioni legali?

I siti di frode non mostrano informazioni di contatto oppure mostrano indirizzi falsi o caselle postali. Mancano le informazioni legali obbligatorie o queste sono falsificate.

CONTROLLI PRIMA DI ISCRIVERSI N. 3

Gli utenti hanno la possibilità di caricare contenuti sul sito?

Un indicatore di illegalità è la possibilità per gli utenti di caricare contenuti che non sono auto-prodotti.

Dichiarano di essere legali o danno consigli su come essere raggiunti se bloccati?

Il blocco da parte dei fornitori di servizi Internet, le false dichiarazioni di legalità e gli elenchi di server proxy per aggirare i blocchi del sito sono un segno di illegalità.

Il sito è bannato dagli elenchi dei motori di ricerca o si trova nella lista nera dei portali di segnalazione?

Se un motore di ricerca ha bloccato il sito o un watchdog di internet lo segnala come pericoloso, accertatevene prima di registrarvi!

CONTROLLI PRIMA DI ISCRIVERSI N. 4

C'è un qualche pulsante del tipo ordina ora? Il sito offre informazioni sui costi?

Secondo la legge europea i siti web devono chiarire i costi al cliente e offrire ai consumatori una soluzione tramite pulsante per confermare la conclusione di un contratto commerciale.

Esiste un modo per contattare l'assistenza clienti?

L'assistenza clienti - se fornita dal sito web - non è raggiungibile. Se nessuno risponde alla vostra richiesta, non abbonatevi!

Utilizzate la carta di credito o i servizi di pagamento online!

In questo modo, nel peggiore dei casi, potrete utilizzare il servizio di chargeback o il supporto clienti del servizio di pagamento. E anche gli operatori otterranno meno informazioni personali su di voi.

CI SIETE CASCATI?
COSA FARE ADESSO?

Non pagate nulla!

Spesso le fatture dei truffatori sono formulate in modo aggressivo, da un sedicente avvocato o da una fasulla agenzia di riscossione dei pagamenti. Non fatevi intimidire da questo atteggiamento!

Informate le autorità in materia di criminalità informatica!

Segnalate la vostra esperienza alla polizia e al servizio di blacklist su internet, in modo che altri possano essere avvertiti.

Contattate
l'ufficio locale dell'ECC
per un consiglio!

Se non siete sicuri che le richieste di risarcimento siano legittime o che il sito a cui vi siete appena iscritti sia legale, chiedete consiglio al vostro ufficio ECC locale.

fonti: 1 ECC Net

15 years ECC-Net

European Consumer Centre Network

Ulteriori informazioni sulla rete ECC qui.

F & M A

Trova ulteriori informazioni su FAMA qui.

MARCHIO
Data di pubblicazione **Giugno 2020**
Responsabile del progetto/autore **ECC Austria**
Gra ica **Christina Zettl /** buero41a.at

European Consumer Centre Austria
Mariahilfer Straße 81, A-1060 Wien
www.europakonsument.at
www.facebook.com/europakonsument.at
E-Mail: info@europakonsument.at

Questa pubblicazione è stata finanziata dal Programma consumatori dell'Unione Europea (2014-2020).

Co-funded by the European Union

LA NOSTRA MISSIONE Una rete di 30 Centri europei di consumatori (ECC) consente ai consumatori di conoscere i loro diritti e di sfruttare appieno le opportunità offerte dal mercato unico.

COME PORTIAMO A TERMINE LA NOSTRA MISSIONE Gli esperti legali della rete ECC assistono gratuitamente i consumatori nella risoluzione dei loro problemi transfrontalieri, fornendo una solida consulenza legale. La rete offre una panoramica unica e informazioni affidabili sulle questioni relative ai consumatori nel mercato interno che possono essere utilizzate per l'elaborazione di politiche in collaborazione con le parti interessate europee e nazionali.

Film & Music Austria (FAMA) **ha offerto supporto per quanto riguarda la traduzione di contenuti e testi.**

DICHIARAZIONE DI NON RESPONSABILITÀ Il contenuto di questa pubblicazione illustra esclusivamente il punto di vista dell'autore ed è di sua esclusiva responsabilità; non può essere considerato come espressione del punto di vista della Commissione Europea e/o dell'Agenzia esecutiva per i consumatori, la salute, l'agricoltura e la sicurezza alimentare (CHAFEA) o di qualsiasi altro organismo dell'Unione Europea. La Commissione europea e l'Agenzia non si assumono alcuna responsabilità per l'uso che può essere fatto delle informazioni in essa contenute. Responsabilità per i link: Il materiale informativo contiene link a siti web esterni di terzi. Il rispettivo fornitore o gestore dei siti è responsabile del contenuto dei siti collegati. Le offerte legali menzionate sono esempi documentati dei principali attori del mercato. La loro menzione non costituisce un'approvazione dei prodotti/servizi da essi offerti.