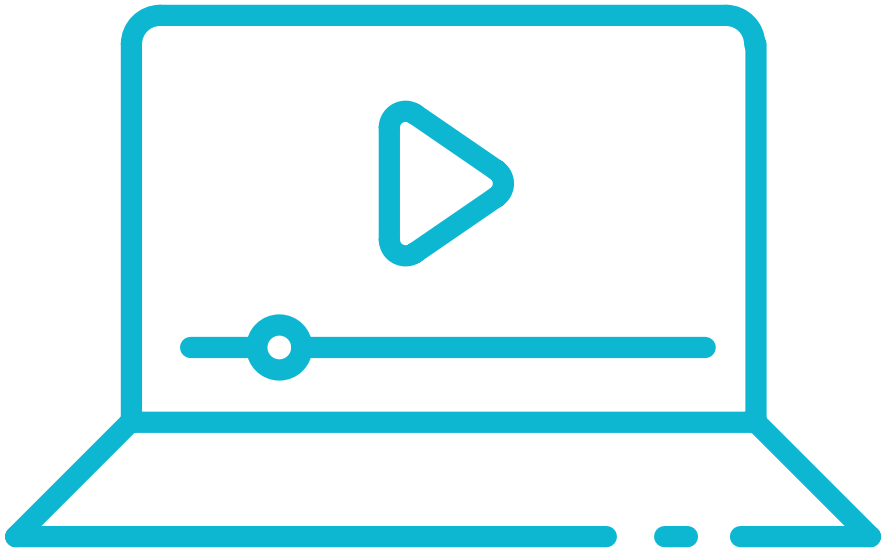
15 years ECC-Net

European Consumer Centre Network

ECC NET - June 2020
in cooperation with F & M A



SAFER STREAMING

Threats from illegal video on demand services and what you can do about it

INDEX

03 **Streaming is Booming**
04 **Two Systems of Video on Demand Services**
05 **Fake vs Illegal**

FAKE STREAMING SITES
06 **Help, I'm Trapped!**
07 **They'll Abuse Your Data**
08 **Manipulating Your Device**

ILLEGAL SITES
09 **Selling Stolen Content**
10 **No Youth Protection**

11 **Fully Loaded and Jailbroken – what´s that?**
12 **Uploading and Sharing**
13 **Social Media and Illegal Streams**
14 **Useful to Know**

APPENDIX
15 **Dos & Don'ts**
21 **Disclaimer & Imprint**

STREAMING IS BOOMING

The convenience of viewing your favorite program at your own leisure on any device makes video streaming services the new standard for modern consumers.

In the last years, streaming technology has changed the media landscape fundamentally by successfully merging the online and television worlds. With this profitability, many streaming companies are able to spend more than the classic film industry to produce[1] exclusive TV series and films, growing their audience even more.

60%

of global downstream internet traffic is video[2]

42%

more streaming subscriptions in Europe every year[3]

89%

of millennials are streaming[4]



Today's majority of global internet bandwidth is consumed by streaming. During the Corona crisis in spring 2020 it surged to such an extent, that the EU Commission urged leading providers to reduce video quality to ensure internet speed for more important services such as web meetings for home office.[5]

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

TWO SYSTEMS OF VOD SERVICES

Video on Demand lets you watch whatever you want, whenever you want and, with a properly connected mobile device, also wherever you want without the need to download content by watching a data stream. You can connect by using a smart TV, computers of all sorts, smartphones, tablets and even gaming consoles.

IPTV "INTERNET PROTOCOL TELEVISION"

Established broadcasting companies that deliver signals by cable or satellite now offer internet-based TV too. Most viewers receiving IPTV content through their broadband internet connection have set top boxes or smart TVs and pick from an electronic program guide. Sporting events, live broadcasts, and the news remain the backbone of more conventional television networks now available live or on demand.



OTT "OVER THE TOP" SERVICES

When it comes to streaming, this usually refers to OTT companies, both local and Europe-wide, such as Netflix, Amazon Prime or Sky/NOW TV.[1] Such services can be delivered to any connected device, independent from your internet service provider or any dedicated broadband network. Extensive libraries of TV series and movies are a major draw for customers. New, original and exclusive productions are also very attractive.

sources: 1 EAO yearbook

FAKE VS ILLEGAL

Illegal downloads of pirated material have decreased in recent years[1], because users prefer to use safe, convenient and reasonably priced sites instead of risking sources that could result in downloading infected files, combined with the risk of prosecution by law enforcement.

Legitimate streaming sites are financed by advertising, rental and subscription models. Illegal deviations of this business have grown into a constant threat and increasingly replace older kinds of piracy. Another issue is scam sites just pretending to offer subscriptions or content.

SCAM SITES



Trap inexperienced consumers in fake subscriptions and abuse their personal data.

PIRATE SITES



Try to appear legitimate to lure users into watching or buying stolen content (while stealing their private information).

sources: 1 EUIPO

FAKE STREAMING SITES –

HELP, I'M TRAPPED!

A common trick of scammers is to present an unsuspicious front page with pictures or trailers of tempting media content accessible in a brief free trial period.



Once you have registered you will discover that you cannot access the promised content after all. Since you did not pay anything you may think there is no damage done and are likely to ignore it.

A few days later an invoice demanding several hundred euros for a yearly subscription will reach you, stating that the free trial transforms into a yearly subscription automatically after the testing period of a few days is over.

FAKE STREAMING SITES –

THEY'LL ABUSE YOUR DATA

Most scam streaming websites do not host **any content at all.**



Hundreds of such sites follow the same template and are set up across Europe, often by the same criminals. After some time they disappear if they receive more warnings or if shut down by law enforcement - making the fraudulent domain less profitable. The sites reappear shortly after under new domain names, starting a new round of scamming.

In addition to selling fake subscriptions these sites make profit from phishing: **selling personal data entered by users during registration.**[1]

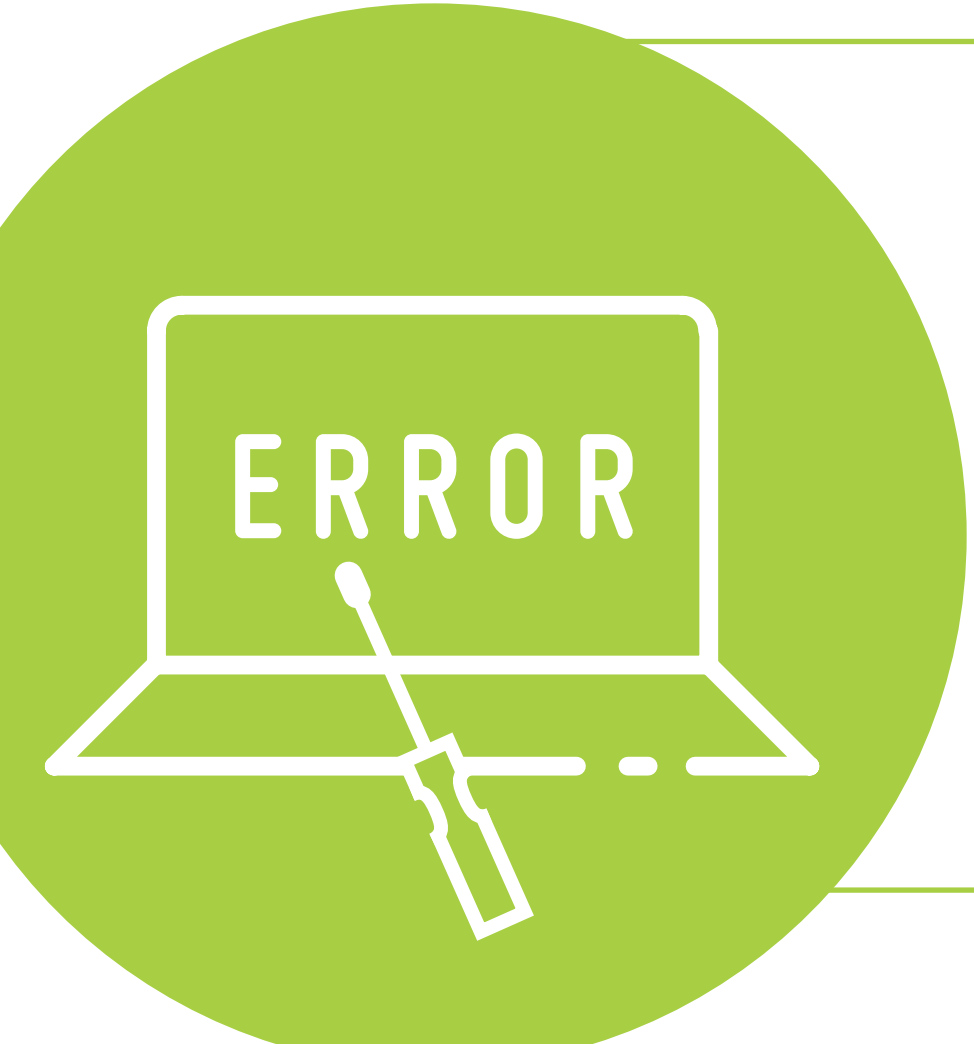
Some fake sites even send out personal messages by email or SMS after registration, claiming to require further personal data for security reasons. All the data is collected to be sold, often to other criminal **ventures**

Source: 1 Europol

FAKE STREAMING SITES –

MANIPULATING YOUR DEVICE

Another income source for scammers is advertising. Aggressive pop-up ads may appear on screen. They often show dubious content, are programmed to be hard to get rid of, and clicking them away generates profit for the operator. Either by trying to remove the ads, fake error messages **or, most commonly, installing faked** viewer software **or** codec **to enable watching the promised content, users are twenty-eight times[1] more likely to infect their device with viruses and malware such as:**



PUP **- potentially unwanted programs, annoying and useless software slowing your device**

ADWARE **- showing intrusive advertising coming out of nowhere**

MALWARE **- harmful software giving away your data or abusing your device´s resources**

SCAREWARE **- showing fake error messages or faking prosecution notices by authorities, accusing you of having done something illegal and demanding fine payment or charges for technical assistance**

RANSOMWARE **– encrypting data in your system and blackmailing you for regaining access**

VIRUSES AND TROJANS **– destroying your device system or stealing personal data such as contacts or secretly enabling backdoor access to your system**

Source: 1 IP Crime Threat Assessment 2019

ILLEGAL SITES –

SELLING STOLEN CONTENT





Different to fake sites, illegal sites enable users to watch content but they provide stolen copyrighted material **which takes rightful revenue away from creative content makers and taxpayers whilst nurturing the associated cybercrime scene. Using such sites harms the general public!**

Users may also come across combinations of pirate and fake sites. Such sites pretend to have a big library and lure customers into subscription by showing some streaming for free. The complete catalogue is a fraud in such cases and the limited trial content helps to delay victims realizing and stopping their payments early.

Illicit websites try to look as legitimate as possible **to potential customers. When the illegal nature is not obvious, more people use their service.**

Sometimes it is not easy to identify an illegal site right away as user interfaces of legitimate platforms are copied. Of the top 100 global companies, 46 were found to have at least one brand advertisement on a copyright-infringing website.[1] Criminals know that ads from known brands make their portal look more plausible.

Source: 1 Europol

ILLEGAL SITES –

NO YOUTH PROTECTION

Criminals do not care about protecting children from harmful content. Teenagers and children have not developed healthy boundaries **and are especially vulnerable whilst** using their mobile **devices most** excessively.[1] **They are impulsive and do not understand legitimacy of content. The fact that 56% of all websites[2] are English only does not help the matter. Illegal sites often feature pornographic or other disturbing content, or advertise gambling or betting services, all of which is completely unsuitable for younger audiences. Illegal sites do not prevent underage registrations.**

1of 3

internet users is a child[2]



1of 2

of 11-16 year olds have encountered common internet risks[3]

Parents can check betterinternetforkids.eu **for advice**

Sources 1 IZI study 2 UNICEF 3 LSE study

FULLY LOADED AND JAILBROKEN – WHAT´S THAT?

Pirated content is not limited to OTT technology, but is also an issue in IPTV. There are illicit hardware devices that are harmful for several reasons. So-called **Kodi** boxes are media player attachments to upgrade a smart TV to a fully fledged media center. **“Fully loaded“** versions of Kodi are being sold with manipulated capabilities to stream additional pirated streams from illegal IPTV sources.

Hazards originate from manipulated electronically unsafe **devices.[1] They often are cheap imitations of the original, as in the case of *Amazon Firesticks*, imported from the Far East. Such dealers also often are removed from online trading platforms such as *eBay* before placed orders are delivered.**

Jailbroken devices **have had limits disabled by an operating system and** are no longer covered by warranty**. If there are technical problems, makers and sellers will refuse to fix or refund. The jailbreaking attempt can** lock the owner **out of the operating system, rendering a device useless.**

Illicit hardware can carry malware **and leave a backdoor open to** hacking **into your home network.**



Customers buying illegal devices risk losing money whenever Europol shuts down illegal providers **or if those services stop out of fear of law enforcement. Customs officers or market regulators can confiscate orders of illicit hardware en route. In the case of police action, uploaders can get into legal trouble if they are identified in databases of confiscated servers.**

Sources 1 SBRCentre

UPLOADING AND SHARING

Content found on sharing platforms is mostly protected by copyright laws. **Distribution** without permission is a **violation of copyrights and terms of use.** Uploading protected content without permission is considered illegal.



Ripping **is when streams on screen are recorded and saved in files. Sites offering this possibility will deceive you with claims of being legal, but courts disagree.[1] Usage of download or screen recording tools or uploading copyrighted content is forbidden in the terms of use on legal platforms and violation can lead to a** loss of the user account.

Access your country's comprehendible copyright[2]



Many OTT users share their accounts with friends and family. Over 66 percent of Netflix users share passwords, **resulting in 2.5 viewers per account.[3] For now, OTTs have not undertaken steps against this phenomenon for marketing reasons, but this could change.**

Source: 1 IFPI 2 EUIPO 3 Global Web Index

SOCIAL MEDIA AND ILLEGAL STREAMS

Besides marketing possibilities with 3 billions of users on social media, criminals are exploiting its main characteristic – the share ability. Links to where illegal content is hosted or illicit streams are being posted increasingly, and especially pirated live sports casts reach huge audiences.[1]

New full-length films, series or sports broadcasts are not available legally on these unofficial channels. Owners of content take action against illegal streams on social media and video sharing platforms. This may lead to deletion of user accounts if streaming was shared without permission. Even if it is only for personal use.



The internet makes using and sharing data and content possible on an unprecedented scale and that's great, but everyone has a right to decide for themselves if, when and how to share their own content. Note that this will not change with the new Copyright Directive[2] you may have heard about.

Source: 1 Irdeto 2 Directive EU 2019/790

USEFUL TO KNOW

There are many legal offers and illegal downloads have decreased since offers are getting better and more easily available every day. Apart from the mainstream OTT providers you can check out these links for platforms respecting copyrights:



general: agorateka.eu

sports: sroc.info

music: pro-music.org

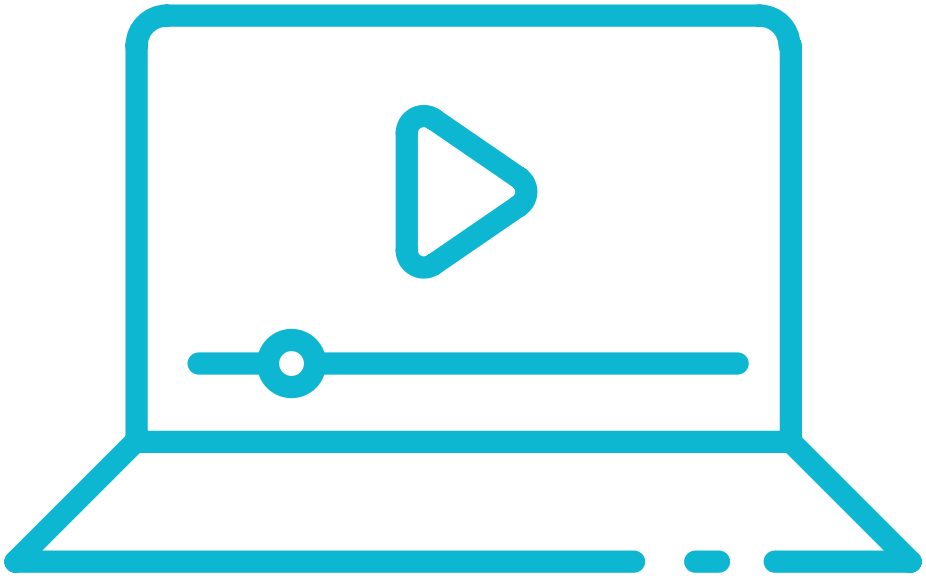
Streaming Apps **allow you to finish watching a running stream on a different device. This comes in handy when travelling and unable to finish watching a movie in one go.**



Since the portability directive[1] **applies in all EU member states, your streaming subscriptions must be provided to you regardless of your location inside the EU. There is no longer a surcharge or prevention to use your streaming service abroad whilst on EU territory.**

Source: 1 EU Commission

APPENDIX



DOS & DON'TS

HAVE A THOROUGH LOOK BEFORE YOU SIGN UP!



Don't enter sites with a bad reputation!

If you search for streaming sites and find something interesting, do not instantly sign up. Invest another minute to check reviews and warnings.



Do they feature unreleased content?

The advertised movie is still in cinemas and they already have it before any other established streaming platform? This is fishy!



Compare the offer with established competitors!

Is it incomparably cheaper than other platforms? A whole year subscription for a very low price or other too-good-to be-true offers?

CHECKS BEFORE SIGN UP #2



Are there text errors?

Scam sites are made from generic templates in different languages. Spelling or grammar mistakes indicate dubious origin.



Is there betting, pornographic or VPN advertising on the site, maybe shown in annoying popups?

Dubious offers often come combined. Legal sites won't abuse excessive pop-up advertisement.



Look for clues! Is there an imprint? Are there terms of service and other legal info?

Scam sites show no contact information, or display fake or letterbox addresses. They lack or fake obligatory legal information.

CHECKS BEFORE SIGN UP #3



Are users allowed to upload to the site?

An indicator of illegality is the option for users to upload content that isn't self-made.



Do they claim to be legal, or give advice on how to be reached if blocked?

Blocking by internet service providers, hollow claims of legality and listings of proxy servers to circumvent site blocks are a sign of illegality .



Is the site banned in search engine listings or blacklisted in warning portals?

If a search engine banned the site or an internet watchdog warns about it, find out before you register!

CHECKS BEFORE SIGN UP #4



Is there some sort of order now button? Does the site inform you about costs?

By European law websites must clarify costs to customer and offer a button solution for consumers to confirm the conclusion of a commercial contract.



Is there a way to contact customer support?

Customer support - if provided on the website at all - is not reachable. If nobody answers your inquiry, do not subscribe!



Use credit card or online payment services!

This allows you to use chargeback or payment service customer support in worst case. Also operators get less personal information about you.

ALREADY TRAPPED? WHAT TO DO NOW?



Do not
pay anything!

**Often scammer invoices are worded aggressively, by a self-proclaimed lawyer or payment collection agency.
Don't get intimidated by that!**



Tell your cybercrime
authority about it!

Report your experience to the police and internet blacklisting service so others can be warned.



Contact your
local ECC office[1]
for advice!

If you´re unsure if claims are legitimate or the site you just subscribed to is a scam ask your local ECC office for advice.

Source: 1 ECC Net

15 years ECC-Net

European Consumer Centre Network

Find further information on the ECC-Net here.

F & M A

Find further information on FAMA here.

IMPRINT
Date published **June 2020**
Project lead/author **ECC Austria**
Graphics **Christina Zettl /** buero41a.at

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

This publication was funded by the European Union's Consumer Programme (2014-2020).

Co-Funded by the European Union

OUR MISSION

The network of 30 European Consumer Centres (ECCs) empowers consumers to know their rights and to take full advantage of the opportunities the Single Market offers.

HOW WE ACCOMPLISH OUR MISSION

The ECC-Net's legal experts assist consumers to solve their cross-border problems free of charge by providing strong legal expertise. The network offers a unique overview and reliable information about consumer affairs in the Internal Market which can be used for policy making in collaboration with European and national stakeholders.

Film & Music Austria (FAMA) **provided support with regard to content and text translations.**

DISCLAIMER

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency (CHAFEA) or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.

Liability for links: **The information material contains links to external websites of third parties. The respective provider or operator of the sites is responsible for the contents of the linked sites. The legal offers mentioned are documented examples of major market players. Their mention is not an endorsement of the products/services they offer.**