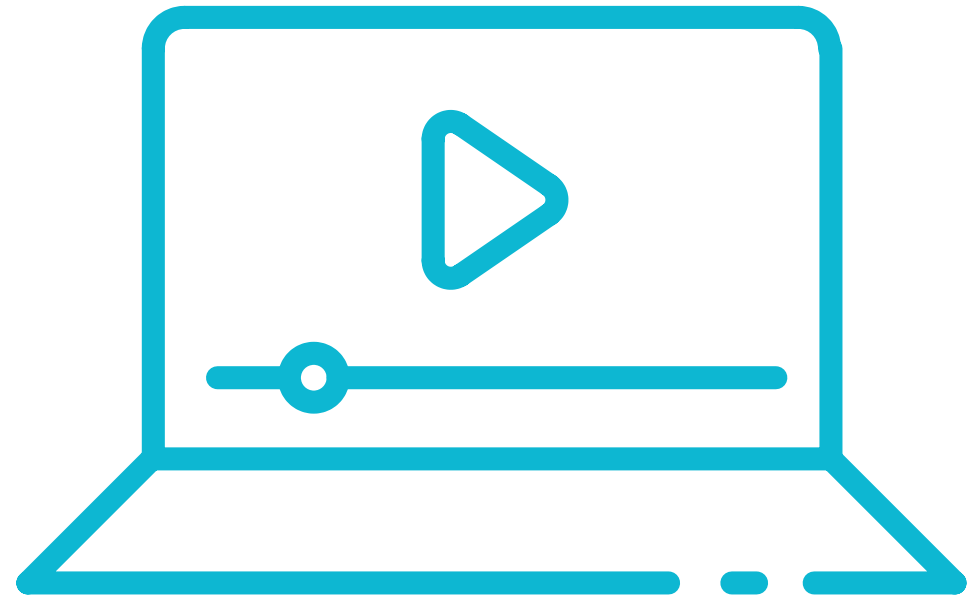




European
Consumer
Centre
Network

EVZ-Netz - Juni 2020
in Zusammenarbeit mit



SAFER STREAMING

Bedrohungen durch illegale Video-on-Demand-Dienste und was man dagegen tun kann

-
- 03 **Streaming boomt**
 - 04 **Zwei Systeme von Video-on-Demand-Diensten**
 - 05 **Gefälschte vs. illegale Streaming-Seiten**
-

GEFÄLSCHTE STREAMING-SEITEN –

- 06 **Hilfe, ich sitze in der Abofalle fest!**
 - 07 **missbrauchen Ihre Daten**
 - 08 **manipulieren Ihr Gerät**
-

ILLEGALE SEITEN –

- 09 **verkaufen gestohlene Inhalte**
 - 10 **sind schädlich für Kinder und Jugendliche**
-

- 11 **Fully Loaded und Jailbreak – was ist das?**
 - 12 **Hochladen und Teilen**
 - 13 **Soziale Medien und illegale Streams**
 - 14 **Gut zu wissen**
-

ANHANG

- 15 **Verhaltensregeln**
 - 21 **Haftungsausschluss & Impressum**
-

DAS STREAMING BOOMT

Die Annehmlichkeit Lieblingsinhalte nach Belieben und auf jedem gewünschten Gerät ansehen zu können hat Videostreaming-Dienste bei modernen Verbraucher als neuen Standard etabliert.

Durch die erfolgreiche Verschmelzung von Internet und Fernsehen hat die Streaming-Technologie die Medienlandschaft in den letzten Jahren grundlegend verändert. Durch diese profitable Verbindung sind

viele Streaming-Anbieter in der Lage, mehr Geld als die klassische Filmindustrie für die Produktion exklusiver TV-Serien und -Filme auszugeben und so noch mehr Zuschauer an sich zu binden.¹

60%

des weltweiten Datenstroms hin zu Nutzern ist Video-Streaming²

42%

mehr Streaming-Abos in Europa jedes Jahr³

89%

der Millennials benutzen Streaming-Dienste⁴

Der Großteil der globalen Internet-Bandbreite wird heutzutage durch das Streaming in Anspruch genommen. Während der Corona-Krise im Frühjahr 2020 stieg die Nutzung rasant an, sodass die EU-Kommission die führenden Streaming-Anbieter dazu drängte, die Videoqualität zu reduzieren, um die Internetgeschwindigkeit für wichtigere Dienste wie Online-Meetings im Home-Office sicherzustellen.⁵



ZWEI SYSTEME VON VOD-DIENSTEN

Mit **Video on Demand** kann man sich ansehen, was man will, wann man will und, solange die Internetverbindung des mobilen Geräts ausreicht, auch von wo immer man will, ohne dass Inhalte heruntergeladen werden müssen. Die Daten werden einfach nur gestreamt. Die Verbindung kann über einen Smart TV, verschiedenste Computer, Smartphones, Tablets und sogar Spielkonsolen aufgebaut werden.

IPTV

„INTERNET PROTOCOL TELEVISION“

Etablierte Fernsehsender, die Signale über Kabel oder Satellit übertragen, bieten jetzt auch internetbasiertes Fernsehen an. Die meisten Zuschauer, die IPTV-Inhalte über ihren Breitbandanschluss empfangen, haben Set-Top-Boxen oder Smart TVs mit einem elektronischen Programmführer (EPG). Sportveranstaltungen, Live-Übertragungen und Nachrichten bilden nach wie vor das Rückgrat konventionellerer Fernsehsender, die mittlerweile live oder in der Mediathek abgerufen werden können.



OTT

„OVER THE TOP“ MEDIENDIENSTE

Wenn man von Streaming spricht, werden damit gewöhnlich sowohl lokale als auch europaweite OTT-Anbieter gemeint, wie z. B. Netflix, Amazon Prime oder Sky/NOW TV.¹ Solche Dienste können von jedem verbundenen Gerät empfangen werden, unabhängig vom Internetanbieter oder Breitbandnetz. Ein umfangreiches Fernsehserien- und Filmangebot zieht die Kunden an. Zudem sind neue, eigenständige und exklusive Produktionen sehr attraktiv.

GEFÄLSCHTE VS. ILLEGALE STREAMING-SEITEN

JUNI
2020

Illegale Downloads von raubkopiertem Material sind in den letzten Jahren zurückgegangen, weil die Benutzer die Nutzung von sicheren, bequemen und preisgünstigen Webseiten vorziehen, anstatt es zu riskieren, ggf. infizierte Dateien herunterzuladen und deshalb eventuell strafrechtlich verfolgt zu werden.¹

Legitime Streaming-Seiten werden durch Werbung, Miet- und Abo-Modelle finanziert. Illegale Abweichungen von diesem

Geschäftskonzept haben sich zu einer ständigen Bedrohung entwickelt und ersetzen zunehmend ältere Formen der Piraterie. Ein weiteres Problem

sind Betrugsseiten, die nur vorgeben, Abos oder Inhalte anzubieten.

BETRUGSSEITEN



locken unerfahrene Verbraucher mit gefälschten Abos in die Falle, um zusätzlich zu Abbuchungen personenbezogenen Daten zu missbrauchen.

PIRATERIE-SEITEN



versuchen, legitim zu erscheinen und verleiten Benutzer dazu, sich gestohlene Inhalte anzusehen oder zu kaufen (und stehlen dabei personenbezogene Daten).

HILFE, ICH SITZE IN DER ABOFALLE FEST!

Ein Standard-Trick von Betrügern ist der unverdächtige Internetauftritt, mit Vorschaubildern oder verlockenden Videovorschauen auf Inhalte, welche in einem kurzen, kostenlosen Testabonnement zugänglich gemacht werden sollen.




Ist man erstmal registriert, merkt man ganz schnell, dass man gar nicht auf die versprochenen Inhalte zugreifen kann. Da man nichts bezahlt hat, denkt man sich schnell, dass kein Schaden entstanden ist und vergisst die Sache.

Einige Tage später kommt dann die Rechnung über hunderte von Euro für ein Jahresabonnement mit der Erklärung, das kostenlose Testabonnement habe sich nach Ablauf einiger Tage automatisch in ein Jahresabo verwandelt.

GEFÄLSCHTE STREAMING-SEITEN -

SIE WERDEN IHRE DATEN MISSBRAUCHEN

Die meisten gefälschten Streaming-Seiten bieten **überhaupt keine Inhalte** an.



Hunderte solcher Seiten folgen dem gleichen Muster und wurden überall in Europa eingerichtet, oft stecken jedoch die gleichen Kriminellen dahinter. Nach einiger Zeit verschwinden sie wieder, wenn sich Warnungen über sie häufen oder Ermittlungsbehörden diese sperren, denn das macht die betrügerischen Domains weniger rentabel. Die Seiten tauchen kurz darauf unter neuen Domainnamen auf und der Betrugs-Spuk fängt wieder von vorne an.

Neben dem Verkauf gefälschter Abos profitieren diese Seiten auch vom Phishing: dem Verkauf personenbezogener Daten, die bei der Registrierung eingegeben werden.¹

Einige gefälschte Seiten versenden nach der Registrierung sogar persönliche Nachrichten per E-Mail oder SMS, wobei sie vorgeben, aus Sicherheitsgründen weitere personenbezogenen Daten abfragen zu müssen. Solche Daten werden nur gesammelt, um verkauft zu werden, und zwar oft an andere kriminelle Betreiber.

GEFÄLSCHTE STREAMING-SEITEN -

MANIPULATION IHRES GERÄTS

Eine weitere Einnahmequelle für Betrüger ist die Werbung. Aufdringliche Pop-Up Werbung kann auf dem Bildschirm erscheinen. Sie zeigen oft dubiose Inhalte und sind so programmiert, dass sie schwer loszuwerden sind, und beim Wegklicken dem Betreiber Gewinn verschaffen. Beim Versuch

der Benutzer, Werbung oder gefälschte Fehlermeldungen loszuwerden, oder am häufigsten beim Installieren angeblicher Software oder eines Codec zum Abspielen der versprochenen Inhalte, ist die Wahrscheinlichkeit achtundzwanzigmal höher, dass Benutzer ihr Gerät mit Viren und Malware infizieren:¹



PUP - potenziell unerwünschtes Programm, lästige und nutzlose Software, die Ihr Gerät verlangsamt

ADWARE - aufdringlich angezeigte Werbung, die plötzlich auftaucht

MALWARE - Schadsoftware, die Ihre Daten klaut oder die Ressourcen Ihres Geräts missbraucht

SCAREWARE - zeigt gefälschte Fehlermeldungen oder Mitteilungen von Behörden mit

der Anschuldigung, Sie hätten etwas Illegales getan und müssten eine Strafe oder Gebühren für technischen Support bezahlen

RANSOMWARE - Daten in Ihrem System werden verschlüsselt und Sie werden erpresst, um wieder Zugriff zu erhalten

VIREN UND TROJANER - zerstören Ihr Betriebssystem oder stehlen persönliche Daten wie Kontakte oder Öffnen eine Hintertür mit Zugriff auf Ihr System

VERKAUF VON GESTOHLLENEN INHALTEN



Im Gegensatz zu gefälschten Webseiten zeigen illegale Seiten den Nutzern Inhalte mit gestohlenem, urheberrechtlich geschütztem Material an, bringen Kreativwirtschaft und Steuerzahler um rechtmäßige Geldmittel und fördern zugleich die damit verbundene Cyberkriminalität. Die Nutzung solcher Seiten schadet der Allgemeinheit!

Benutzer können auch auf Kombinationen von Piraterie-Seiten und gefälschten Seiten stoßen. Solche Seiten geben vor, ein großes Angebot zu haben, und locken Kunden in eine Abofalle, indem einige Streams kostenlos angeschaut werden können. Der Umfang des Angebots ist in solchen Fällen nur vorgetäuscht und der begrenzte Inhalt der Testversion trägt dazu bei, dass Opfer es nicht rechtzeitig erkennen und Zahlungen nicht vorzeitig einstellen.

Illegale Seiten versuchen, potenziellen Kunden einen möglichst legitimen Eindruck zu vermitteln. Ist der illegale Charakter nicht offensichtlich, nutzen mehr Menschen den Dienst.

Manchmal ist es nicht einfach, eine illegale Seite gleich zu erkennen, da die Benutzeroberflächen von regulären Plattformen kopiert werden. Von den Top 100 globalen Unternehmen hat sich bei 46 herausgestellt, dass sie mindestens eine Markenwerbung auf einer Webseite geschaltet hatten, die das Urheberrecht nicht achtet. Kriminelle wissen, dass Werbung bekannter Marken ihr Portal seriöser erscheinen lässt.

KEIN JUGENDSCHUTZ

Der Schutz von Kindern vor schädlichen Inhalten interessiert Kriminelle nicht. Jugendliche und Kinder missachten oft gesunde Grenzen und sind besonders anfällig, indem sie ihre mobilen Geräte sehr intensiv nutzen. Sie agieren impulsiv und verstehen nicht, ob Inhalte angemessen sind oder nicht. Die Tatsache, dass 56 % aller

Seiten ausschließlich auf Englisch angeboten werden, verschärft die Problematik. Illegale Seiten enthalten oft pornografische oder andere beunruhigende Inhalte oder werben mit Glücksspiel- oder Wettangeboten, was für ein jüngeres Publikum völlig unangemessen ist. Illegale Seiten verhindern die Registrierung durch Minderjährige nicht.¹

1 von 3

Internetnutzern ist ein Kind²



1 von 2

der 11 bis 16-Jährigen waren häufigen Risiken im Internet bereits ausgesetzt³

Eltern finden Rat und Unterstützung auf betterinternetforkids.eu

FULLY LOADED UND JAILBREAK – WAS IST DAS?

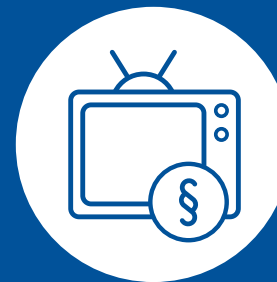
Raubkodierte Inhalte beschränken sich nicht nur auf die OTT-Technologie sondern betreffen auch IPTV. Es gibt gesetzeswidrige Hardware-Geräte, die aus verschiedenen Gründen Schaden anrichten. Sogenannte Kodi-Boxen sind Media-Player, mit denen ein Smart TV zu einem vollwertigen Media-Center aufgewertet werden kann. „Fully loaded“, also vollständig geladene Versionen von Kodi werden mit manipulierten Funktionen verkauft, um zusätzliche raubkodierte Streams von illegalen IPTV-Quellen anzuzapfen.

Manipulierte, elektronisch unsichere Geräte sind häufig eine Gefahrenquelle. Oft sind es billige Nachbauten des Originals, wie bei aus Fernost importierten Amazon Firesticks. Auch werden solche Händler oft von Online-Handelsplattformen wie eBay entfernt, bevor Bestellungen geliefert werden.

Bei Jailbreak-Geräten wurden Funktionen im Betriebssystem deaktiviert und sind nicht mehr von der Herstellergarantie abgedeckt. Wenn es technische Probleme gibt, verweigern Hersteller oder Verkäufer Reparatur oder Rückerstattung. Ein Jailbreak-Versuch kann Besitzer des eigenen Gerätes aus dem Betriebssystem

aussperren, wodurch es unbrauchbar wird.

Illegale Hardware kann Malware enthalten und Hackern Zugriff in ihr Heimnetzwerk geben.



Der Kauf illegaler Geräte wird zum Verlust, nachdem Europol illegale Anbieter deaktiviert hat oder wenn diese aus Angst vor der Strafverfolgung eingestellt werden. Der Zoll oder Marktaufsichtsbehörden können Bestellungen von gesetzeswidriger Hardware auf dem Postweg beschlagnahmen. Kommt es zu einem Polizeieinsatz, können Uploader rechtlich belangt werden, wenn sie in Datenbanken von sichergestellten Servern identifiziert werden.



DAS UPLOADEN (HOCHLADEN) UND SHAREN (TEILEN)

Inhalte, die man auf Tauschplattformen findet, sind größtenteils durch Urheberrechtsgesetze geschützt. Die **Weitergabe** ohne Genehmigung stellt eine **Verletzung der Urheberrechte und Nutzungsbedingungen** dar. Das Hochladen geschützter Inhalte ohne Genehmigung wird als illegal erachtet.



Rippen **bedeutet das Mitschneiden von Streams auf dem Bildschirm und Abspeichern als Dateien**. Seiten, die diese Möglichkeit anbieten, täuschen mit der Behauptung, sie seien legal, doch sind die Gerichte da anderer Meinung. Die Verwendung von Download- oder

Bildschirmaufnahme-Tools oder das Hochladen urheberrechtlich geschützter Inhalte ist in den Nutzungsbedingungen legaler Plattformen verboten, und eine solche Verletzung kann die Deaktivierung des Benutzerkontos nach sich ziehen.¹

Lesen Sie Näheres zum Urheberrecht² in Ihrem Land in verständlicher Sprache



Viele OTT-Kunden teilen ihre Konten mit Freunden und der Familie. Mehr als 66 Prozent aller Netflix-Benutzer geben ihre Passwörter weiter, was 2,5 Zuschauer pro Konto

ausmacht. Bislang haben OTT Anbieter aus Marketinggründen keine Maßnahmen gegen dieses Phänomen getroffen, doch das könnte sich noch ändern.³

SOZIALE MEDIEN UND ILLEGALE STREAMS

Abgesehen von den Marketingmöglichkeiten auf sozialen Medien mit 3 Milliarden Nutzern, machen sich Kriminelle die Haupteigenschaft dieser zunutze: die Funktion, etwas zu **teilen**. Links zu illegalen Streamingangeboten oder illegalen Streams selbst werden vermehrt weitergegeben. Vor allem unrechtmäßige Live-Sportübertragungen erreichen ein sehr großes Publikum.¹

Neue Spielfilme, Serien oder Sportübertragungen sind auf diesen inoffiziellen Kanälen nicht auf legalem Weg erhältlich. Die Eigentümer von Inhalten gehen gegen illegale Streams auf Social Media- und Video-Sharing-Plattformen vor. Dies kann zur Löschung von Benutzerkonten führen, wenn der Stream ohne Genehmigung geteilt wurde. Selbst dann, wenn es nur für den persönlichen Gebrauch ist.



Das Internet macht die Nutzung und den Austausch von Daten und Inhalten in einem noch nie dagewesenen Ausmaß möglich, was einerseits natürlich großartig ist. Doch hat jeder das Recht, selbst zu entscheiden, ob, wann und wie eigene Inhalte mit anderen geteilt werden. Wir weisen darauf hin, dass sich dies mit der neuen Urheberrechtsrichtlinie, von der Sie vielleicht schon gehört haben, nicht ändern wird.²

GUT ZU WISSEN

Es gibt viele legale Angebote und die Anzahl illegaler Downloads ist zurückgegangen, seit die Angebote immer mehr verbessert und einfacher zugänglich werden. Zusätzlich zu den bekannten OTT-Anbietern könnten Sie auch einen Blick auf folgende Plattformen werfen, auf denen die Urheberrechte respektiert werden:



Allgemeines:

agorateka.eu

Sport:

sroc.info

Musik:

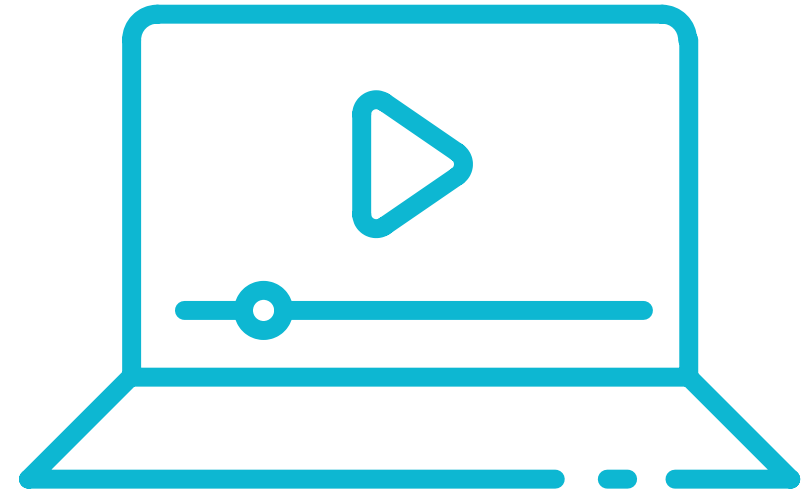
pro-music.org

Streaming-Apps **machen es leicht, einen begonnenen Stream auf einem anderen Gerät fortzusetzen.** Das ist praktisch, wenn man auf Reisen ist und sich einen Film nicht ohne Unterbrechung ansehen kann.



Da die Portabilitätsrichtlinie **in allen EU-Mitgliedsstaaten gilt, müssen Ihnen Ihre Streaming-Abonnements unabhängig von Ihrem Standort innerhalb der EU zur Verfügung gestellt werden.** Es wird kein Zuschlag mehr erhoben bzw. die Nutzung Ihres Streaming-Dienstes wird nicht mehr verhindert, wenn Sie sich im EU-Ausland aufhalten.¹

ANHANG



VERHALTENS- REGELN

SCHAUEN SIE VOR DER ANMELDUNG GANZ GENAU HIN!



Besuchen Sie keine
Seiten mit
zweifelhaftem Ruf!

Wenn Sie nach Streaming-Seiten suchen und etwas Interessantes finden, melden Sie sich nicht sofort an. Nehmen Sie sich eine Minute Zeit, um nach Kommentaren und Warnungen zu suchen.



Sind unveröffentlichte
Inhalte enthalten?

Der beworbene Film ist noch in den Kinos und die Seiten haben ihn bereits vor jeder anderen etablierten Streaming-Plattform? Das ist äußerst fragwürdig!



Vergleichen Sie das
Angebot mit dem von
bewährten Anbietern!

Ist es um einiges billiger als andere Plattformen?
Ein ganzes Jahresabo zu einem sehr niedrigen Preis oder andere Angebote, die zu gut sind, um wahr zu sein?

VOR DER ANMELDUNG ABKLÄREN – TEIL 2

JUNI
2020



Gibt es Fehler
im Text?

Betrugsseiten werden aus einer gleichen Vorlage in verschiedenen Sprachen erstellt. Rechtschreib- oder Grammatikfehler weisen auf eine dubiose Herkunft hin.



Wird auf der Seite
Werbung für Wetten,
Pornografie oder VPN
angezeigt, gegebenenfalls
als nervige Pop-ups?

Fragwürdige Angebote werden oft kombiniert. Auf legalen Seiten gibt es keine übermäßige Pop-up-Werbung.



Suchen Sie nach Indizien!
Gibt es ein Impressum?
Sind Nutzungsbedingungen
und andere rechtliche
Informationen vorhanden?

Betrugsseiten zeigen unwahre oder unvollständige Kontaktinformationen oder Briefkastenadressen an. Vorgeschriebene Rechtshinweise fehlen dort oder sind gefälscht.

VOR DER ANMELDUNG ABKLÄREN – TEIL 3

JUNI
2020



Dürfen Nutzer
Inhalte auf der Seite
hochladen?

**Können Nutzer fremde - also nicht selbst
erstellte Inhalte - hochladen, dann handelt es
sich wahrscheinlich um einen illegalen
Anbieter.**



Stehen Behauptungen da,
legal zu sein, oder gibt es
Tipps, wie man die Seite im
Falle einer Sperrung
erreichen kann?

**Seitensperren durch Internetanbieter,
übertriebene Betonung legal zu sein, und
Listen von Proxy-Servern zur Umgehung von
Seitensperren deuten auf Gesetzeswidrigkeit hin.**



Wird die Seite bei der
Googlesuche oder in
anderen Suchmaschinen
nicht angezeigt oder wird sie
auf Warnlisten geführt?

**Wenn eine Suchmaschine die Seite blockiert
oder ein Sicherheitsportal davor warnt, sollten
Sie das vor und nicht erst nach dem Anmelden
herausgefunden haben!**

VOR DER ANMELDUNG ABKLÄREN – TEIL 4

JUNI
2020



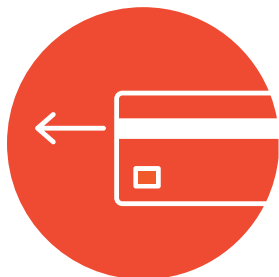
Gibt es eine Schaltfläche, über die man die Bestellung bestätigen muss? Werden die Kosten angezeigt?

Nach europäischem Recht müssen Webseiten Kunden beim Bestellvorgang den Preis anzeigen und einen Button zum Abschluss des Geschäftsvertrages haben.



Gibt es einen Kundenservice?
Ist dieser erreichbar?

Der Kundenservice – sofern auf der Seite überhaupt angeführt – kann nicht erreicht werden. Wenn niemand auf Ihre Anfrage antwortet, schließen Sie kein Abo ab!



Verwenden Sie eine Kreditkarte oder einen Online-Zahlungsdienst!

So können Sie im schlimmsten Fall Rücklastschriften oder den Kundenservice von Zahlungsdiensten in Anspruch nehmen. Die Betreiber erhalten so auch weniger personenbezogene Daten von Ihnen.

BEREITS IN DER ABOFALLE? UND JETZT?



In die Falle
getappt? Nichts
bezahlen!

Oft werden die betrügerischen Rechnungen von einem angeblichen Anwalt oder Inkassobüro aggressiv formuliert. Lassen Sie sich davon nicht einschüchtern!



Melden Sie den
Vorfall der für
Cyberkriminalität
zuständigen Stelle.

Melden Sie Ihre Erfahrung der Polizei und Warnseiten im Internet, damit andere Personen nicht in dieselbe Falle tappen.



Lassen Sie sich vom
**Europäischen
Verbraucherzentrum**¹
in Ihrem Land beraten!

Wenn Sie gerade ein Abo abgeschlossen haben und unsicher sind, ob deren Forderungen rechtens sind oder ob die Webseite betrügerisch vorgeht, fragen Sie beim EVZ nach.



European
Consumer
Centre
Network

Mehr Informationen zum ECC-Net finden Sie [hier](#).



Mehr Informationen zu FAMA finden Sie [hier](#).

Impressum

Veröffentlichungsdatum **Juni 2020**
Projektleiter/Verfasser **EVZ Österreich**
Grafik **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

Diese Veröffentlichung wurde aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014-2020) finanziert.



Co-funded by the
European Union

UNSER AUFTRAG

Das Netzwerk der 30 Europäischen Verbraucherzentren (ECC-Net) informiert Verbraucherinnen und Verbraucher über ihre Rechte in Europa und stärkt sie darin, die Vorteile des Binnenmarktes voll auszuschöpfen.

SO ARBEITEN WIR

Das Netzwerk der Europäischen Verbraucherzentren (kurz: ECC-Net) unterstützt Verbraucherinnen und Verbraucher durch sein fundiertes juristisches Fachwissen kostenlos bei grenzüberschreitenden Verbraucherangelegenheiten. Es verfügt über langjährige Erfahrung und bietet zuverlässige Informationen zu Verbraucherfragen im europäischen Binnenmarkt. Diese Expertise des Netzwerks kann in Zusammenarbeit mit nationalen und europäischen Interessenvertretern für Verbraucherpolitik genutzt werden.

Film & Music Austria (FAMA) **unterstützte diese Publikation inhaltlich und bei Übersetzungen.**

HAFTUNGSAUSSCHLUSS

Der Inhalt dieser Veröffentlichung gibt nur die Ansichten des Verfassers wieder und liegt in seiner alleinigen Verantwortung; es kann nicht davon ausgegangen werden, dass er die Ansichten der Europäischen Kommission und/oder der Exekutivagentur für Verbraucher, Gesundheit, Landwirtschaft und Ernährung (CHAFEA) oder eines anderen Organs der Europäischen Union widerspiegelt. Die Europäische Kommission und die Agentur übernehmen keine Verantwortung für die Verwendung der darin enthaltenen Informationen.

Haftung für Links: Die Publikation enthält Links zu externen Webseiten Dritter. Für Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Bei den genannten rechtlichen Angeboten handelt es sich um dokumentierte Beispiele von führenden Unternehmen. Ihre Erwähnung sollte nicht als Befürwortung der von ihnen angebotenen Produkte/Dienstleistungen herangezogen werden.