PRESSEINFORMATION

Wien, 15. Juni 2020

Europäisches Verbraucherzentrum Österreich

Das EVZ Österreich warnt vor unseriösen Video-Streaming-Angeboten

Betrugsversuche führen zu einer erhöhten Anzahl von Verbraucherbeschwerden

Schon vor der Coronavirus-Pandemie befand sich der Markt für Streaming-Angebote in einem soliden Wachstumsprozess. Die Lockdown-Maßnahmen zur Eindämmung von COVID-19 haben die Nachfrage noch einmal zusätzlich boomen lassen, sodass sich führende Streaming-Dienste auf Bitten der EU-Kommission zwischenzeitlich sogar bereit erklärten, die Videoqualität der Streams zu reduzieren, um Bandbreite für wichtigere Dienste freizuhalten. Auch wenn sich der erste Ansturm von Neukunden auf die Streaming-Plattformen bereits etwas gelegt hat, die erhöhte Nachfrage im Bereich Video-Streaming hat auch zu einer erhöhten Anzahl von Konsumentinnen und Konsumenten geführt, die auf betrügerische Angebote hereingefallen sind. Viele Verbraucher bemerken es nicht, wenn sie sich bei einem unseriösen Streaming-Dienst angemeldet haben. Das böse Erwachen kommt oft erst einige Tage später, wenn Schreiben von Anwälten oder Inkassobüros eintreffen, die mehrere hundert Euro für angeblich abgeschlossene Jahresmitgliedschaften fordern. Aufgrund der zahlreichen Hilfeanfragen von Geschädigten hat das im Verein für Konsumenteninformation (VKI) angesiedelte Europäische Verbraucherzentrum Österreich (EVZ) jetzt unter www.europakonsument.at/streamen Informationen zum Thema Video-Streaming zusammengestellt.

Konsumentinnen und Konsumenten, die im Internet nach Streaming-Angeboten für TV-Serien oder Filme suchen, finden neben bekannten Marktführern oft auch unbekannte Webseiten mit besonders günstigen Angeboten. Nicht selten entpuppen sich solche Angebote als unseriös. Folgende betrügerische Vorgehensweisen werden häufig angewendet:

Viele dieser Webseiten täuschen schlichtweg etwas vor, was sie nicht sind: Kunden registrieren sich, geben ihre persönlichen Daten preis und erhalten dafür im Gegenzug nichts, weil es die angepriesenen Videos in der vorgetäuschten Mediathek gar nicht gibt. Solche Webseiten werden oft nur mit dem Ziel des Daten-Phishings eingerichtet. Zusätzlich zu den Einnahmen durch die Weitergabe der erbeuteten Daten finanzieren sich diese kriminellen Internetauftritte auch durch das Schalten aggressiver Werbung.

Andere Webseiten bieten zusätzlich eigene Streaming- oder Player-Software zum Download an. Dies richtet oft große Schäden an, wenn Kunden sich, um die vermeintlichen Streams ansehen zu können, als Abspielsoftware getarnte Computerviren oder Malware in ihrem System installieren.

Zudem kommt es häufig zu aggressiv formulierten Geldforderungen für angeblich abgeschlossene Abonnements oder Mitgliedschaften, denen die Konsumenten auf keinen Fall nachkommen sollten. Da die Nachfrage nach Streaming-Diensten dermaßen groß ist, reicht es den Tätern, wenn pro zehntausend Aufrufen einige Opfer den Einschüchterungen nachgeben, um großen Profit aus solchen kriminellen Domains zu ziehen.

Ein weiteres Problem sind illegale Streaming-Plattformen, die das Copyright im großen Stil missachten und so Raubkopien oder gestohlene Sportübertragungen zu Dumpingpreisen verbreiten und dabei persönliche Daten stehlen. Die so entgangenen rechtmäßigen Einnahmen finanzieren dann stattdessen weitere illegale Aktivitäten und schädigen die Allgemeinheit.

Das Europäische Verbraucherzentrums Österreich empfiehlt zum Schutz vor unseriösen Anbietern:

- Nehmen Sie sich bei der Auswahl eines Streaming-Anbieters Zeit und lassen Sie sich nicht vorschnell durch Gratisversprechen leiten. Vergleichen Sie die Angebote mit anderen etablierten Anbietern. Wenn die Tarife unrealistisch günstig sind, sich Kundenrezensionen mit Beschwerden betrogener Kunden im

Web finden lassen oder Filme angeboten werden, die noch in den Kinos laufen, sollten Sie besser von dem Angebot Abstand nehmen und andere Anbieter wählen.

- Achten Sie darauf, ob die Webseite einen seriösen Eindruck macht und formale Regeln einhält: Gibt es viele Textfehler auf der Webseite? Erscheinen das Impressum und Nutzungsbedingungen glaubwürdig? Werden aggressive Pop-Up-Banner oder anzügliche Werbung eingesetzt? Wird die Domain zu einer anderen Internetadresse umgeleitet? Wenn dies zutrifft, ist das Angebot vermutlich nicht seriös.

- Ein weiteres Anzeichen für betrügerische Angebote ist der Umgang mit Nutzungsrechten: Wird häufig versichert, dass es sich um ein legales Angebot handelt? Gibt es Anleitungen, wie man die Seite über Proxyserver erreichen oder Ländersperren umgehen kann? Haben Suchmaschinen die Seite aus den Trefferlisten gelöscht? Hat ein Warndienst die Seite auf seine schwarze Liste gesetzt? Können Nutzer fremde Videos hochladen?

- Sollten Sie sich für einen Anbieter entscheiden, achten Sie vor und während des Anmeldeprozesses auf folgende Punkte: Existiert ein Kundenservice? Prüfen Sie es durch einen Testanruf. Gibt es einen Button, mit dem man zahlungspflichtig bestellt und werden dabei die Kosten angezeigt, wie es gesetzlich vorgeschrieben ist? Nutzen Sie für die Bezahlung sicherheitshalber eine Kreditkarte oder einen Online-Bezahldienst. Dadurch geben Sie weniger Daten preis und können bei Bedarf eine Rücküberweisung durch den Zahlungsabwickler veranlassen.

Was tun, wenn man bereits in eine Falle getappt ist?

Bezahlen Sie nichts, auch wenn die Forderung mit Drohungen versehen ist! Bei Unsicherheit über die Rechtmäßigkeit einer Forderung können Sie beim EVZ nachfragen. Berichten Sie Ihre Erfahrungen an die Meldestellen für Computerkriminalität, damit andere Personen vor Betrügern gewarnt werden.

SERVICE: Weitere Informationen zu diesem Thema finden Sie auf www.europakonsument.at/streamen.

RÜCKFRAGEHINWEIS: Europäisches Verbraucherzentrum, Pressestelle, Tel.: 01/588 77-256,
E-Mail: presse@europakonsument.at