Steam Архів відмов у наданні підтримки та стандартних відповідей — Досьє «Steam»

Джерело: https://phishdestroy.io/steam_dossier/uk/support_canned_refusals
CC0 1.0 Universal · 2026-09-30

ЩО ДОКАЗУЄ ЦЕЙ РОЗДІЛ
У цьому репозиторії містяться збережені оригінальні скріншоти з сайту 137 та перевірені звернення потерпілих з сайту 1,505, в яких детально описано процес автоматизованої обробки запитів до служби підтримки на сайті Valve. Це доводить, що у випадках, коли облікові записи зламують через перенаправлення OpenID або несанкціоноване генерування ключів API, служба підтримки Steam систематично використовує стандартні шаблонні відмови без проведення технічного розслідування. Категорично відмовляючи у відновленні предметів або наданні даних аудиторського сліду, платформа перекладає повну відповідальність за системні недоліки аутентифікації на власників зламаних облікових записів.

Усі скріншоти є знімками, зробленими сторонніми особами. Авторські права та зміст належать відповідним авторам та платформам (користувачам Reddit, авторам спільноти «Steam», рецензентам Trustpilot, авторам публікацій на сайтах X та YouTube). Вони відтворені виключно з метою ідентифікації та висвітлення питань, що становлять суспільний інтерес; жодних прав власності на них не заявляється. Кожен матеріал містить посилання на першоджерело.

Figures reported on the source page

Measure	Reported value	Scope
Документальні записи	1505	Перевірені звернення потерпілих та теми про штрафи
Збережені знімки екрана	137	Знімки квитків у високій роздільній здатності, збережені локально
Коефіцієнт відновлення	0.0%	Скасування рішень у справі «API» — викрадення літаків
Дублювання шаблонів	100%	Повторне використання дослівних сценаріїв різними співробітниками (Ілля, Роджер, Маверік)

Судово-медичні докази: три основні підстави для відмови у наданні допомоги

ПІЛАР 01 · ВСТУП Додаток R —014

The Roger Admission: Підтверджено атаку «людина посередині» (MitM) на API

У відповіді на звернення №1ср582і співробітник служби підтримки Steam на ім’я «Роджер» письмово визнає, що зловмисники скасовують законні угоди через сайт API і замінюють їх на клоновані боти за мілісекунди, але відмовляється відновити предмети та радить потерпілому звернутися до «місцевого комп’ютерного фахівця».

Переглянути письмове підтвердження зарахування ↗
ПІЛАР 02 · ЕСКАЛАЦІЯ Додаток R —012

7-Денна торгівля: утримання позиції, відсутність дій

Одна з жертв надала SteamID64 акаунтів хакера під час періоду блокування торгівлі в рамках акції «7-». Співробітники служби підтримки «Артем» та «Ілля» відмовилися заблокувати вкрадені предмети, посилаючись на їхню рідкість, і закрили запит, використавши автоматичний шаблон.

Переглянути виписку з даних про персонал ↗
ПІЛАР 03 · ПОЛІТИКА Додаток R —002

Дефіцит на ринку у зв’язку з правами власності

В офіційній Політиці повернення предметів Valve чітко зазначено, що предмети не підлягають поверненню, оскільки їхнє повернення «зменшило б їхню рідкість та спричинило б інфляцію в економіці, що призвело б до зниження вартості предметів на Спільнотному ринку».

Переглянути знімок екрана з умовами політики ↗
Історичне походження · 22 Березень 2018 на 2026
Додаток H —003 · 8-: Площа атаки без виправлень за рік

Найдавніший зафіксований випадок заміщення товарів (22 березня 2018)

Рівно за тиждень до того, як компанія «Valve» запровадила суперечливе обмеження на денну торгівлю предметами в грі «Counter-Strike» — так зване «7-», — торговельна спільнота виявила перші реальні випадки **Steam Експлойт, пов’язаний з перенаправленням у веб-API**. Зловмисники перехопили веб-сесії, щоб згенерувати несанкціонований ключ API на `steamcommunity.com/dev/apikey` без підтвердження з боку мобільного додатка 2FA, що дозволяє ботам скасовувати та обмінювати угоди в режимі реального часу.

Попередження від громадської організації «2018» за березень: *«Шахраї можуть автоматично виявити цю пропозицію обміну й відхилити її у вашому акаунті, оскільки у них є ваш ключ Steam API. Тепер шахрайський бот надішле вам пропозицію обміну тими самими скінами... і ви навіть не помітите різниці!»*
Історичний маршрут
22 Березень 2018: Перший задокументований випадок заміни двигуна «API»
2019: Підтримка стандартизує відбивання «шкідливого програмного забезпечення»
2020: Посилено захист скрипта «Закрити запит на допомогу»
2022–2026: Автоматизація фішингових атак з використанням BitB та QR-кодів
Відкрити оригінальну гілку на Reddit «2018» ↗

Primary sources

137 gallery cards refer to 78 distinct primary URLs. Images and repeated exhibit captions are omitted from this reading edition.

Full visual archive and original captures