Steam Lưu trữ các trường hợp từ chối hỗ trợ và câu trả lời mẫu — Hồ sơ “Steam”

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

PHẦN NÀY CHỨNG MINH ĐIỀU GÌ
Kho lưu trữ này ghi lại các ảnh chụp màn hình gốc được lưu giữ tại 137 và các đơn khiếu nại của nạn nhân đã được kiểm toán tại 1,505, trong đó nêu chi tiết quy trình xử lý phiếu hỗ trợ tự động của Valve. Điều này chứng minh rằng khi các tài khoản bị xâm phạm thông qua chuyển hướng OpenID hoặc việc tạo khóa API trái phép, bộ phận Hỗ trợ của Steam đã có hệ thống sử dụng các mẫu từ chối chuẩn hóa mà không tiến hành điều tra kỹ thuật. Bằng cách từ chối một cách dứt khoát việc khôi phục vật phẩm hoặc tiết lộ nhật ký kiểm toán, nền tảng này chuyển toàn bộ trách nhiệm pháp lý về các lỗ hổng xác thực mang tính cấu trúc sang cho chủ sở hữu các tài khoản bị xâm phạm.

What this means — OpenID and openid.realm
OpenID is the sign-in standard behind the “Sign in with Steam” button: the site does not receive the password, Steam confirms the identity to it. **openid.realm** is the field carrying the address of the site asking for the sign-in, and **openid.return_to** the address Steam is to send the user back to. Steam receives both on every request and prints the realm on its own login page — which is why this dossier can name the host each platform authenticates through.

Section 3 — the observed routes →

Tất cả các ảnh chụp màn hình đều là các bản chụp do bên thứ ba thực hiện. Bản quyền và nội dung thuộc về các tác giả và nền tảng tương ứng (người dùng Reddit, các tác giả của cộng đồng Steam, người đánh giá trên Trustpilot, X và những người đăng tải trên YouTube). Các ảnh chụp màn hình này được sao chép lại chỉ nhằm mục đích nhận diện và đưa tin vì lợi ích công cộng; chúng tôi không tuyên bố sở hữu bất kỳ quyền nào đối với chúng. Mỗi tài liệu minh họa đều có liên kết đến nguồn gốc ban đầu của nó.

Figures reported on the source page

Measure	Reported value	Scope
Hồ sơ được lưu trữ	1505	Các bài đăng khiếu nại của nạn nhân đã được xác minh và các chuỗi bài về vé
Các ảnh chụp màn hình được lưu giữ	137	Bản chụp vé độ phân giải cao được lưu trữ cục bộ
Tỷ lệ phục hồi	0.0%	Các quyết định hủy bỏ đã được ban hành trong các vụ chiếm đoạt tàu chở dầu mang tên “API”
Sao chép mẫu	100%	Tái sử dụng kịch bản nguyên văn giữa các nhân viên (Ilya, Roger, Maverick)

Chứng cứ pháp y: Ba trụ cột chính của việc từ chối hỗ trợ

TRỤ CỘT 01 · TUYỂN SINH Tài liệu R-014

Lời thừa nhận của Roger: Xác nhận vụ tấn công MitM trên API

Trong phản hồi yêu cầu hỗ trợ số1cp582i, Steam, nhân viên hỗ trợ “Roger” thừa nhận bằng văn bản rằng những kẻ tấn công hủy các giao dịch hợp lệ thông qua API và thay thế chúng bằng các bot giả mạo chỉ trong vài mili giây, nhưng từ chối khôi phục các vật phẩm và yêu cầu nạn nhân tìm đến một “kỹ thuật viên máy tính địa phương”.

Kiểm tra giấy nhập học ↗
TRỤ CỘT 02 · THẨM QUYỀN XỬ LÝ Tài liệu R-012

7-Giao dịch trong ngày – Giữ vị thế – Không thực hiện hành động nào

Một nạn nhân đã cung cấp SteamID64 của các tài khoản thuộc về hacker trong khoảng thời gian tạm ngưng giao dịch trong ngày của sự kiện “7-”. Nhân viên hỗ trợ “Artem” và “Ilya” đã từ chối khóa các vật phẩm bị đánh cắp, với lý do vật phẩm ảo này rất hiếm, và đã đóng phiếu yêu cầu bằng một mẫu trả lời tự động.

Xem bảng điểm của nhiều nhân viên ↗
TRỤ CỘT 03 · CHÍNH SÁCH Tài liệu R-002

Tình trạng khan hiếm trên thị trường so với quyền sở hữu tài sản

Chính sách hoàn trả vật phẩm chính thức của Valve nêu rõ rằng vật phẩm sẽ không được hoàn trả vì việc hoàn trả chúng sẽ “làm giảm tính khan hiếm và thổi phồng nền kinh tế, từ đó làm giảm giá trị của các vật phẩm trên Thị trường Cộng đồng”.

Xem ảnh chụp màn hình Chính sách ↗
Nguồn gốc lịch sử · 22 Tháng 3 năm 2018 đến 2026
Phụ lục H -003 · 8-Diện tích tấn công chưa được vá trong năm

Trường hợp thay thế hàng hóa được ghi chép sớm nhất (22 March 2018)

Chính xác một tuần trước khi Valve áp dụng quy định gây tranh cãi về thời gian chờ 7-đối với các vật phẩm trong Counter-Strike, cộng đồng giao dịch đã phát hiện những trường hợp đầu tiên trên thực tế về việc **Steam Lỗ hổng khai thác chuyển hướng giao dịch trên trang web API**. Những kẻ tấn công đã chiếm quyền điều khiển các phiên truy cập web để tạo ra một khóa API trái phép tại `steamcommunity.com/dev/apikey` không cần xác nhận từ ứng dụng di động 2FA, cho phép các bot hủy và hoán đổi giao dịch theo thời gian thực.

Thông báo cảnh báo của PSA tháng 3 năm 2018: *"Những kẻ lừa đảo có thể tự động phát hiện đề nghị giao dịch này và sẽ từ chối nó trên tài khoản của bạn, bởi vì chúng có khóa Steam API của bạn. Lúc này, bot lừa đảo sẽ gửi cho bạn một đề nghị giao dịch với những skin tương tự... và bạn sẽ không nhận ra sự khác biệt nào cả!"*
Con đường Dấu vết Lịch sử
22 2018: tháng 3 Lần đầu tiên được ghi nhận về việc hoán đổi API
2019: Hỗ trợ tiêu chuẩn hóa việc ngăn chặn “phần mềm độc hại”
2020: Tăng cường bảo mật cho tập lệnh "Đóng yêu cầu trợ giúp"
2022–2026: Tự động hóa lừa đảo qua BitB và mã QR
Mở chủ đề gốc trên Reddit về “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