

Section 3.2

The Big Picture Trap: Multi-Year Longitudinal Phishing Audit (120 Domains)

Investigated by: Agent Ignatus

The Big Picture Trap: Multi-Year Longitudinal Phishing Audit (120 Domains)

The Big Picture Trap: Link Filter is Compliance Theater, Not a Shield

On desktop browsers, users are shielded by external defenses: Google Safe Browsing and Microsoft SmartScreen intercept known phishing with full-screen red warnings. **Inside Steam's Big Picture mode, the in-game overlay (Shift+Tab), and the Steam Deck (SteamOS), those defenses do not exist.** The embedded browser supports zero extensions, disables external Safe Browsing engines, and leaves the user with exactly one defensive barrier: Valve's linkfilter interstitial.

Swipe to compare all four results →

92.5%

2025–2026 modern edge phishing **passed clean** (37/40)

77.5%

2023–2024 CS2 era phishing **passed clean** (31/40)

70.0%

2021–2022 legacy phishing **passed clean** (28/40)

7 / 7

gambling mains blocked (positive control)

Multi-Year Longitudinal Audit: 120 Pure Steam Phishing Domains Tested Live (24 Sep 2026)

To test whether Valve's filter is simply slow to ingest new threats or fundamentally blind to them, we audited **120 confirmed Steam-specific phishing domains** across three historical cohorts against `steamcommunity.com/linkfilter`:

- **Cohort 1: 2021–2022 (Classic Trade-Offer & Item Drops) — 70.0% Clean Pass (28/40).** Even 4 to 5 years after being cataloged by community watchdogs, 7 out of 10 legacy phishing hosts still open without any block.
- **Cohort 2: 2023–2024 (CS2 Beta Hype & Fake Support Appeals) — 77.5% Clean Pass (31/40).** Campaigns impersonating Counter-Strike 2 releases and fake community appeals (e.g. `cs2-steam.com`, `appealsteamcommunity.help`) pass straight through.
- **Cohort 3: 2025–2026 (Serverless Edge Deploys & Favicon Clones) — 92.5% Clean Pass (37/40).** Modern phishing kits deploying on EdgeOne, Vercel, and Cloudflare Pages (e.g. `steamgifter.online`, `steam-dp4lt5b8fnez.edgeone.dev`) pass virtually unobstructed.

Telemetry & Liability Shield, Not Protection. Why does the Link Filter exist if it passes 70% to 92.5% of pure Steam phishing? It functions as a corporate liability disclaimer and an outbound click telemetry sensor. By presenting a polite *"You are leaving Steam"* notice with a clickable green proceed button, Valve shifts legal blame onto the victim under the Steam Subscriber Agreement ("the user voluntarily navigated outside Steam"). Valve collects the telemetry of the click, but does not block the theft.

The Favicon Hash Proof: Zero Ingestion of Threat Feeds. Independent threat intelligence platforms (`urlscan.io`, Shodan, Censys) identify live Steam phishing kits using a simple search for Steam's official favicon hash (`page.favicon.hash:9f890a9debcdfcc339149a7943be9aff9e4c9203c2fa37d5671a5b2c88503ad NOT domain:*.steampowered.com`). This basic automated check surfaces active phishing clusters in seconds. Valve does not sync with external feeds, does not run hash-based threat hunting, and only manually intervenes when compelled by regulators (the 2016 WSGC gambling order) or to protect its trademarked domain strings.

Primary audit evidence artifacts: Longitudinal 120-domain multi-year audit: [longitudinal-steam-phishing-audit.json](#) · 100 dedicated Steam phishing sample: [linkfilter-steam-phishing-100.json](#) · Broad feed audit (n=250): [linkfilter-coverage-2026-09-22.json](#).

[Download PDF](#)

[Download JSON](#)

[Download PGP signature](#)

PhishDestroy · file integrity signature for this fact

[Material record ↗](#)