License · Rights · Disclaimer — PhishDestroy

Source: https://phishdestroy.io/steam_dossier/license_disclaimer
CC0 1.0 Universal · 2026-10-04

PHISHDESTROY *Forensic investigation · Valve / Steam*
License · Rights · Disclaimer

License & Legal Disclaimer — Public Domain Dedication

All rights surrendered to humanity.

Public rights declaration **CC0 1.0 Universal**
Use · adapt · translate · commercialise

Read the full terms ↓
PhishDestroy gives up every right to this material — reproduce it, sell it, put your name on it. What follows is two documents in one voice's clothing: an open letter to Valve, written the way we actually write, and a formal waiver written for the authority that will carry the substance forward.

One fact. One author. One signature.
This dossier is a collection of individually attributed fragments, compiled by PhishDestroy.

Read the authorship agreement (§5) Open the fragment map — authors, PDFs, JSONs and signatures

Formal register · for the authority

Declaration As to use and rights

PhishDestroy Project & Cybersecurity Coalition

This declaration accompanies every submission and every exhibit in this referral set. It is addressed to any authority, court, regulator, prosecutor, researcher, journalist or affected person into whose hands the material comes.

1. There are no conditions on use

1.1 All material produced by the Coalition in this referral — the statements of fact, the analysis, the exhibits it has authored, the tooling, and the findings — is released WITHOUT RESERVATION OF ANY RIGHTS.

1.2 Anyone may, without asking and without notifying us:

reproduce it, in whole or in part;

adapt, edit, rewrite, restructure or correct it;

translate it;

excerpt it without indicating that it has been excerpted;

incorporate it into official documents, findings, decisions, pleadings, reports or press material;

present it as the recipient's own work or the recipient's own findings;

use it as raw material and discard the rest;

and pass it on to anyone else on the same terms.

1.3 ATTRIBUTION IS NOT REQUIRED AND IS NOT SOUGHT. The Coalition need not be named, cited, credited, thanked, consulted or informed. If material from this referral assists an authority and the Coalition is never mentioned, THAT IS A COMPLETELY SATISFACTORY OUTCOME and the Coalition states so in advance so that the question need not be raised.

1.4 If, on the other hand, an authority finds it more convenient to cite the Coalition as a source, it is free to do so. The choice is entirely the recipient's and neither course carries any consequence.

1.5 This is a WAIVER, not a licence offer. It requires no acceptance, imposes no obligation, and cannot be breached. Software published by the Coalition is separately released under the MIT licence; the research and findings are released into the public domain to the fullest extent permitted, and where a jurisdiction does not permit waiver, the Coalition grants an irrevocable, worldwide, royalty-free licence to the same effect.

2. Why this matters practically, and not only as a courtesy

2.1 An authority may reasonably hesitate to rely on material supplied by an outside party, for fear of appearing to act at that party's instance or of acquiring some entanglement with it.

2.2 THERE IS NOTHING HERE TO BE ENTANGLED WITH. The Coalition asks for nothing, is owed nothing, retains nothing, and has no expectation of any kind. It cannot later assert a right, claim credit, complain of misuse, or object to how the material is characterised, because it has retained no basis on which to do so.

2.3 An authority using this material is therefore not acting for the Coalition. It is using public information that happens to have been assembled by someone else.

3. Everything is open already

3.1 The Coalition's work is public by default:

the investigations are published openly at https://phishdestroy.io and are freely readable;

the tooling is published as open source under the MIT licence at https://github.com/phishdestroy archived 2026-09-11 ↗;

the methodology is set out in the referral itself, at Annex A section A.16D, including the weight and limitations of each source type;

the Coalition accepts no donations and has published that position since 2018.

3.2 The only material NOT published is that which cannot lawfully or safely be published: personal data of victims and of third parties, and information that would expose a source to retaliation. That material is supplied to authorities in confidence and is identified in the schedules of evidence.

3.3 The Coalition invites scrutiny of its own conduct on the same terms it invites scrutiny of anyone else's, and has volunteered its own data handling to the authorities concerned, including a request for a direction on disposal.

4. Integrity of the evidence bundle

4.1 Exhibits are supplied with the submission or, where marked, on request through a secure channel. They are not published at a public address and no such address should be inferred: material of this kind is provided to authorities directly.

4.2 Each delivery is accompanied by a file SHA256SUMS listing a SHA-256 digest for every file supplied, together with a detached OpenPGP signature SHA256SUMS.asc.

4.3 The signing key is published at https://phishdestroy.io/.well-known/pgp-key.txt and on keys.openpgp.org. Its fingerprint appears in the letterhead of every submission in this set.

4.4 Any recipient may verify at any time that a file in their possession is the file that was sent, unaltered:

gpg --verify SHA256SUMS.asc SHA256SUMS

sha256sum -c SHA256SUMS

4.5 The purpose is not formality. It is so that, if the accuracy or integrity of any exhibit is disputed at a later date, the question can be settled by computation rather than by argument.

Compartmentalization of Evidence (The "Agent" Protocol)

To ensure the absolute integrity of this referral and to prevent the dilution of evidence, this dossier is architected as a decentralized aggregate. Every macro-fact or investigation chapter is submitted by an independent, anonymous member of the Coalition (designated for internal tracking as 'Agent [Name]').

Each fragment is individually authored, cryptographically signed, and independently released into the public domain (CC0 1.0 Universal). Consequently, any legal or technical challenge to a specific fragment addresses only that specific author's submission. The invalidation of one fragment by a court or platform does not invalidate the cryptographic, legal, or factual integrity of the remaining aggregate. We are a library of facts, not a monolithic plaintiff.

5. Authorship, Aggregation, and Compartmentalization (The "Agent" Protocol)

5.1 The Coalition acts exclusively as a distributed Wiki-style aggregator. This dossier is not a single monolith; it is a compiled library of independent factual findings and OSINT reports submitted by various independent researchers.

5.2 To ensure absolute evidentiary isolation, this bundle is structurally compartmentalised. Each standalone section, JSON object, and PDF exhibit is assigned to a specific compiler/author. The legal invalidation of any single section has no bearing on the validity of the others.

5.3 To protect the safety of these independent researchers, their real identities are withheld. Instead, each compartment is authored under a specific pseudonym.

5.4 In selecting these pseudonyms, the Coalition has chosen to adopt the exact same nomenclature and anonymity standard designed and historically utilized by Valve Corporation for its own outsourced support staff.

5.5 Therefore, regulatory readers will observe sections authored by "Agent Kal", "Agent Brian", etc. We adopt Valve's corporate standard for anonymity out of respect for their operational security protocols. If Valve's legal counsel wishes to issue a subpoena regarding a specific fact, they must officially file it against "Agent Kal" or "Agent Logen" — challenging their own naming convention on the public record.

1 fact = 1 author = 1 separately signed fragment. Each numbered investigation point has one distinct assigned author. Collected evidence and third-party sources retain their original attribution. The PDF identifies the author and title. The matching JSON includes the author and PDF SHA-256. Its detached OpenPGP signature authenticates file integrity: PhishDestroy signs as the collection compiler, not as the fragment author.

FRAGMENT → AUTHOR → JSON + PDF → DETACHED SIGNATURE

Fragment titles, authors and file index (JSON) · Index signature

Signature and content-integrity checks

The map follows 25 numbered points in the main dossier and 5 numbered points in Part II. Each entry shows the English material title, its Agent author and separate PDF, JSON and signature links. Exhibits are sources, not additional agent-authored documents.

5.6 The fragment map

30 numbered materials. 30 individual authors. The public register identifies each fragment by title and author, with direct PDF, JSON and detached-signature downloads. Translations retain the same author.

Open the fragment map — titles, authors and signed files →

6. On register — why the waiver is functional and not merely generous

6.1 The authority may encounter the Coalition's published investigations and find them blunt, adversarial and at times satirical. That impression is correct. The Coalition writes that way deliberately and does not apologise for it.

6.2 IT ALSO RECOGNISES THAT THIS IS THE WRONG REGISTER FOR A REGULATORY OR JUDICIAL PROCEEDING. A serious matter should not be carried in the voice of a campaign. Findings put before an authority should be stated flatly, with their limitations admitted, and should not require the reader to discount for tone before reaching the substance.

6.3 THAT IS PRECISELY WHY THE COALITION WAIVES AUTHORSHIP. The waiver at section 1 is the mechanism by which the substance can be separated from the register: the authority may take what is useful, restate it in its own voice, and discard every word of the Coalition's manner along with the Coalition's name. Nothing is lost by doing so, and the Coalition would prefer it.

6.4 THE COALITION ALSO ASKS THAT THE REGISTER NOT BE MISTAKEN FOR THE METHOD. The published tone is combative; the underlying practice is not careless. Throughout this referral, inference is separated from observation, testimony is identified as testimony, sources are weighted and their weaknesses stated, figures are presented with their limitations, and points the Coalition cannot prove are put as questions for the authority rather than as assertions. Where the evidence cut against the Coalition's own position it has said so — see Annex A, paragraph 7, and section B.0 of the parallel referral.

6.5 THE COALITION EXPLAINS THE CONNECTION BETWEEN ITS MANNER AND ITS FINANCES BECAUSE THE TWO ARE NOT SEPARABLE. It takes no money from anyone — no donations, no bounties, no clients, no sponsors. That refusal is what makes the bluntness possible: an organisation with revenue to protect must moderate what it says about the parties it depends on. Having nothing to protect, the Coalition has nothing to moderate.

It is also the reason the Coalition continues to exist. There is no other engine. The work is done because it is done; it stops when the people doing it stop.

6.6 The authority need accept none of this. It is stated so that the tone of the Coalition's public work is not read as a measure of the care taken with the material now before it.

7. What the Coalition is providing, in its own words

Information, research and observation.

Nothing is asserted as a finding that the Coalition has no standing to make. Where something is inferred, the referral says so. Where something rests on testimony, the referral says whose and with what limitation. Where the Coalition cannot answer a question, it says that too, and identifies who can.

The Coalition seeks no remedy, no payment, no acknowledgement and no outcome for itself or for any individual. It asks only that the questions set out in the referral be put to Valve Corporation by a body with the power to compel an answer.

Two signed objects · rights and published text

Signed release What is signed, and what it covers

The rights grant and research text are separately signed JSON objects below. Each detached OpenPGP signature authenticates the exact bytes of the JSON named beside it. The rights statement grants permissions; the text snapshot identifies and contains the material being published.

1. Rights statement

`license-rights.json`

Signed object: the complete `license-rights.json` file, containing the public rights grant dated 28 September 2026. It grants permission to copy, publish, edit, translate, combine and commercialise authored dossier materials without attribution, notification or approval. This signature authenticates the rights statement; it does not authenticate the text of every webpage or PDF.

The original signed release is preserved unchanged. Its existing grant cannot be withdrawn or narrowed by changing the website, publishing another file or taking the site offline. Third-party materials retain their own rights.

▼ Verification commands

```
gpg --verify license-rights.json.asc license-rights.json
sha256sum -c license-rights.json.sha256
```

2. Published text

`dossier-text.json`

Signed object: the complete `dossier-text.json` file. It contains the actual readable text of the exported pages in `documents[].content.text`, with each page’s title, language, source URL, source HTML hash, headings and references. The `documents` list is the exact inventory covered by this snapshot; the language variants are listed separately. It is a text publication, not just a list of hashes.

Every entry identifies its lightweight page PDF by filename and SHA-256 in `documents[].pdf`. The JSON also identifies the original rights statement by URL and SHA-256, so the published text, its PDF and the applicable rights release can be matched without guessing. Linked external databases, image originals and pages absent from the inventory are not embedded in this text snapshot.

▼ Verification commands

```
gpg --verify dossier-text.json.asc dossier-text.json
sha256sum -c dossier-text.json.sha256
```

On the dossier home page, the PDF and JSON buttons export the research bundle. On an inner page, they export that page in its published language. Each page JSON also has its own detached signature and SHA-256 file, named explicitly in its `integrity` object. To verify the

associated PDF, calculate its SHA-256 and compare it with the `pdf.sha256` value in the verified JSON. The PDF is bound by that digest; it does not carry a PDF-format digital signature.

3. Printable research bundle

`steam-dossier-{language}.content.json`

Signed object: the complete language-specific JSON file, including the bundled chapter text in `documents[].content.text`, chapter page ranges, source languages, the excluded-source inventory and the exact PDF digest in `pdf.sha256`. The five supplementary evidence archives remain linked online and are not bundled. Authored research text is retained; visual catalogues are replaced with source links.

English
Deutsch
▼ Verification commands

```
gpg --verify steam-dossier-en.content.json.asc steam-dossier-en.content.json
sha256sum -c steam-dossier-en.content.json.sha256
```

Public verification key ↗

Signing fingerprint: 129F C7F3 9C40 C69D 2EF3 C329 BFCF 9E8D D295 EE01

```
gpg --import pgp-key.txt
gpg --fingerprint 129FC7F39C40C69D2EF3C329BFCF9E8DD295EE01
```

Check that the displayed fingerprint matches the one above, then verify the signature against the exact JSON filename. Editing a signed JSON changes the signed object and invalidates its original signature. A valid signature identifies the published bytes; it is not independent verification of the research findings.

The open letter

Our voice. The background.

The original commentary and context, kept alongside the formal declaration.

New subsection · Source 1 **Open response to Source 1** Read the full seven-part response ↗
▼ About this declaration
WHAT THIS SECTION PROVES
This instrument establishes the unconditional public domain dedication (CC0 1.0 Universal) and MIT software licensing terms governing the PhishDestroy Steam Dossier. All forensic findings, evidentiary datasets, network graphs, and analytical methodologies are placed irrevocably in the public domain for unrestricted regulatory, legal, and academic use worldwide.

← Back to Executive briefing
Investigation · Valve Corporation / Steam Public edition — no expiry, no take-backs

Section I License *— the actual legal part, but human*

PhishDestroy gives up every right to this material. Zero. Gone. Done. You can reproduce it, sell it, put your name on it, tattoo it on your boss, whatever. No credit required, no DM needed, no thank-you card expected.

One actual rule (yes, just one)

Access from OFAC-sanctioned jurisdictions is prohibited. That is a matter of territory and law — not of nationality and not of people.

Changing your Steam region does not change your physical location or your legal status. No loopholes.

Section II What this is and why it exists

We will publish more about Valve than an average Valve employee knows about themselves. That's not a brag. That's just where we ended up.

The decision of our contributors to remain anonymous is a strict security protocol, based on the documented history of the controller's legal representatives—a firm whose public record includes the manipulation of electronic evidence in this very case, alongside a widely reported history of internal ethical violations. Our identities are irrelevant to the mathematics of this report.

How did we get here? Funny story: Steam basically created us. It raised us on its scammers, its support tickets, its ban evasion ecosystem — and now here we are. No hard feelings. Poetic, actually.

For those who haven't read the origin story yet — we already met Valve's extremely expensive European lawyers (Taylor Wessing, since you asked):

https://phishdestroy.medium.com/my-dog-vs-elite-gdpr-lawyers-the-valve-data-breach-nobody-is-talking-about-f6f7683d813d archived 2026-08-21 ↗

Charming encounter. Especially given their hourly rate.

Did Valve know? Yes. Did Taylor Wessing know? Almost certainly yes. But when you're that rich, laws are more of a vibe than a requirement, right?

That's kind of the whole answer, actually.

Steam spent years farming scammers. Not always intentionally — sometimes scammers just got Valve's fingerprints on them by association. We're not trying to be dramatic about it. We're trying to be precise. That's harder for us than being dramatic, to be honest — this is just how we write.

Is this a conflict?
— No.

Can it be resolved?
— Yes. But we're not signing any NDA and we're not playing bug bounty for pennies.

We waited over 4 years for them to fix the spoofing issue before we could write about it publicly. Because if we had written about it earlier, Steam would've put on its little victim face and screamed "active threat!" and offered us pocket change to sign a document that would've made us their legal property forever. No thanks.

(Also: Valve itself violates NDA. Their own employees do. The ones near the top. But sure, let's talk about ours.)

Section III Open letter to Valve — *seriously, read this*

Valve: if you want this domain taken down, email us. Outside counsel is not needed for that conversation.

For the uninitiated: Dr. Patrick holds a Master of Laws in International Commercial Law from the University of Aberdeen and — wait for it — literally finished his doctoral dissertation in IT law. He recently made partner at Taylor Wessing, which is a firm whose entire business model is billing companies like Valve obscene amounts of money to drag things out until the other side runs out of money or patience.

We don't blame him. Rich guilty clients who pay by the hour — solid career move. We just don't think you should be funding it.

The deal (open offer, no lawyers needed)

If you want the domain gone, this is the whole offer — no outside counsel required.

If you want the domain gone:

Let your IT law professionals calculate its price. Take your time — it is a rare asset: the only website whose purchase changes nothing, because everything on it already lives on IPFS, in regulator inboxes, and in archives we do not control.

50% of whatever you pay goes to the SEAL Foundation (securityalliance.org) — people who do volunteer security work professionally and publish it for free. We are not affiliated with them and they did not ask for this; we name them as the public standard of what real volunteers look like — the standard your own volunteer moderators and outsourced support failed, publicly, before you had to remove them.

The rest buys the community coffee while we keep publishing.

That is not a settlement offer. It is a demonstration of what money can't reach: the domain is the maximum Valve can obtain, and obtaining it obtains nothing. The referrals continue. The mirrors continue. Part 3 continues.

Will we "damage" Valve directly? Probably not in a way they'll feel fiscally. We're not delusional. But we will do it honestly, openly, without chasing clout — because we don't need clout. We need the world to see what was always publicly visible if you spent enough time looking.

We have 5 years of archives. What Valve's lawyers showed in discovery — the data that support agents can see, the fingerprints, the paper trail they literally handed us — is enough. We don't need to leak it raw.

Who gets what

Regulators get the originals.

Researchers and journalists get redacted versions (victim reports, children's logins and Valve's charming support commentary removed for obvious reasons).

Minors were among the affected accounts and were not notified. That finding sits in the regulator package with the victim reports and credentials removed, because it belongs in front of a data-protection authority rather than in an article.

Also, Valve — we want to make something clear before you decide how to play this: PhishDestroy is a community, not a person. You learned that when you addressed legal correspondence to the community without bothering to speak with the community — just milked it for data and banned the accounts.

The community has no conflict with Valve. We didn't go looking for this. The scammers you grew found us. We blocked them. And here we are.

Section III-B The allied resources — *a note to Steam specifically*

We want to be upfront about the amplification structure, because pretending it doesn't exist would be dishonest.

PhishDestroy, as we understand the community situation, has at least two allied resources that will pick up this material and run with it.

What that means in practice:

They work their own angles on overlapping subject matter.

They are independent — they don't take our direction, we don't take theirs. Same general topic, different methodology.

They will NOT be activating on Part 1. They're watching.

If Valve chooses not to take down the site:

Expect them to surface after Part 2 or Part 3.

They'll take what's useful from our work, supplement it with their own, and publish under their own authorship.

This is exactly the kind of thing the license in Section 1 is built for: the material goes where it needs to go, gets supplemented, gets amplified — and neither we nor they owe each other attribution.

(PS for lawyers wondering about liability chains: there are none. These resources don't receive our direction, our funding, or our data. They read what's public and draw their own conclusions. Just like you could.)

We're not saying this to intimidate. We're saying it so that whoever is strategising on Valve's side has accurate information about what the information environment actually looks like.

One resource that pulls our material and supplements it would be a story. Two resources doing it independently and reaching similar conclusions is a pattern. Patterns are what regulators notice.

Section IV The money, the bans, the whole circus

Here's the thing about Steam banning gambling sites and scammers: it's not enforcement. It's revenue capture. Valve pockets the money, cleans its hands, then goes on stage and tells everyone a wholesome story about Pokémon cards and baseball.

Where support-side compromises are documented — including Valve's written admission in February 2023 taking responsibility for high-value accounts compromised through help requests, and contractor staff dismissals reported by Dexerto and Escorenews following the $320k insider trade (Part II §04 · Main Dossier §14.1) — they rest on published admissions and investigative reporting. Unsubstantiated rumors of support staff operating gambling side hustles or taking percentages to lift bans are unestablished on the public record and are excluded here.

Meanwhile Valve killed the ability to properly track skins in 2017. They even discussed it on their own forums. Called it "anti-gambling measures" — while the skin gambling ecosystem continued to route billions through Steam's infrastructure for years after. Great branding.

We're going to prove that:

Skins are more anonymous than Monero

A Peruvian Cartel allegedly used Dota 2 skins for money movement

Steam is functionally a sanctions-bypass machine worth ~$7B in "trading cards" (yes, they actually said trading cards to a prosecutor)

We've got a video on the skins thing. You'll see it.

We also know:

Reddit moderation is influenced by Valve

Third-party Steam data infrastructure (such as steamid.uk) is operated by a private individual (msart) whose linked sibling ban-list project (steambans.com archive) is co-administered by a confirmed Valve community moderator (killahinstinct_) — leaving independent auditing of platform bans entirely inside Valve's orbit (see Card Economy §08)

What they can't control, they ban

Valve: if you keep playing dumb — that's fine. Your safe harbour is noted. Google Analytics anonymises your users' IPs anyway. We see what gets deleted. We just can't prove it cheaply enough for your lawyers to care. Yet.

Section V The malware thing — *yes, we're mentioning it*

Let's be brutally clear about the sequence of events, because it exposes exactly who you are.

We are NOT disclosing the vulnerability in the game publicly. We are NOT reporting it to Steam. The programme requires an NDA, and signing one would bar us from telling the affected users what happened to their accounts. Disclosure to the people who lost those accounts, and to regulators, is the point of this work; a confidentiality agreement is incompatible with it.

Here's what actually happened: This vulnerability is practically an open secret in the right circles. We know for a fact that independent security researchers have already shoved the full exploit directly into Steam Support's face. That part is done. You have been officially warned through your own sterile channels.

And what did Valve do? Absolutely nothing. Because for Valve, security does not equal profit — in fact, it's the exact opposite. Security is a cost center. Until a threat reaches critical mass and causes a catastrophic public PR meltdown, Valve does not treat it as urgent.

So what are we doing? We're telling the public it exists, because "Valve knows about a systemic malware threat and actively chooses to do nothing" is a critical data point for the regulators currently reading this.

The game is massive. We're not naming it here. But understand this:

This is NOT the trivial CS:GO script-kiddie garbage where a server asks you to "install a driver". This is catastrophic.

This is an Unturned-level nightmare: zero-click RCE on server connect. You join a server. You click nothing. You download nothing. The connection itself is the attack surface, and your machine is fully compromised. Let's be real here: dropping an RCE and bypassing local antiviruses by piggybacking on Valve's trusted digital certificates isn't even a novelty on Steam anymore. It is practically a built-in feature of your ecosystem.

Valve already knows this exists. But they rely on their favorite, cowardly legal loophole: because the game is technically developed by a third party, Valve washes its hands. They distribute the game, they process the payments, they host the infrastructure, but when a zero-click RCE threatens millions of their users, their stance is: "Not our game, not our liability."

When this inevitably blows up, the third-party developer will take the bullet, and Valve will walk away pretending to be the responsible platform that "assisted" with the resolution. Classic Valve cowardice. We've seen the playbook.

We are putting this on the record so that regulators, prosecutors, and journalists understand exactly how Valve handles active malware: by hiding behind third-party developers, deploying NDA gag orders, and leaving the players as sitting ducks.

Closing note To whoever is carrying this forward

We want to thank whoever gets this material to where it needs to go. It's probably not going to be a quick trip. Valve has deep pockets and Taylor Wessing charges by the hour — that combination is specifically designed to make people like you give up before they reach the finish line.

We know what we're doing. We know who we're writing about. Valve built us — how could we not understand them?

PhishDestroy has no conflict with Valve. We blocked the only scammer ring of that scale we've come across — we didn't go looking for a fight with Valve. It just turned out that every road led back to them. Not a conflict. Just topology.

Valve cannot resolve the PhishDestroy situation because there is nothing to resolve. We have no relationship. The data about their enrichment schemes and overflow profits is largely public — you just had to spend enough time to see it. Think of it as a success encyclopedia: "How to Not Follow Sanctions So That Russian Hackers Can't Pirate Our Free Games (The Paid Ones They Won't Pirate Anyway)." You get the vibe.

We don't need authorship.

We don't need attribution.

We don't need a win.

We need someone with actual authority to ask Valve the questions that are already sitting in this referral, with the power to require an answer.

That's it. That's the whole ask.

Cases will live at:

https://steamdestroy.eth/

https://steamdestroy.eth.limo (currently broken — will fix when needed)

We'll be at:

https://phishdestroy.eth.limo/ archived 2026-06-27 ↗

https://phishdestroy.eth/

PhishDestroy — public investigation — all rights surrendered to humanity

OFAC-region access: prohibited