THREAT INTELLIGENCE REPORT

Our Values & Personal Motives

Ref. **PD-TI-2026-92483** Published **10 July 2026** Source **phishdestroy.io/our-values**

The Brutal Truth · Non-commercial · Since 2019
9 min read · Updated **April 2026** · PhishDestroy Intelligence
Why we do this for free. Why that matters. And what it enables us to do that others can't.

The Question Everyone Asks

"Why do you do this for free?"

That's the question we get constantly. From journalists. From security researchers. From scammers trying to understand their enemy. From people who genuinely can't comprehend why anyone would spend years building threat intelligence infrastructure without monetizing it.

So here's the truth — unfiltered, uncomfortable, and exactly what you probably didn't expect.

Collaboration Without Money

There is something most people misunderstand about us: staying free does not mean staying isolated.

We collaborate. We share tools. We help other projects grow. Even paid ones — if they genuinely serve society and weaken the scam ecosystem.

But here's the part that defines us:

We never take a cent for it.

Why Zero Money Makes Collaboration Stronger

Money creates dependency. Dependency creates influence. Influence creates silence. Silence protects scammers.

So we collaborate only on the terms that matter: *no profit, no deals, no financial leverage, no ownership, no obligations.*

We've supported small researchers building tools. We've amplified niche OSINT projects. We've shared intel with analysts building commercial products. We've helped operators, developers, journalists, independent investigators — anyone aligned with the same mission.

No Competition — Only Alignment

We don't compete with anyone. You can't compete with something that refuses to enter the economy in the first place.

PhishDestroy exists to increase the total pressure on scammers, not to own the spotlight.

If another project builds something useful — great. We will promote it. We will support it. We will send people to it. Because the goal isn't to grow *our* power.

The goal is to grow the ecosystem's power against phishing.

We don't profit. We don't sell. We don't monetize. We strengthen whatever helps destroy scam infrastructure — because that's the only metric that matters.
This is why we stay free forever: not to signal virtue, but because the absence of money is the strongest weapon in this war. It keeps us clean, untouchable, unaligned, and impossible to manipulate.

And every collaboration we choose follows one simple rule:

If it helps destroy phishing — we're in. If it requires profit — we're out.

THE CORE TRUTH

We don't take money because money creates restrictions. And restrictions protect scammers.

Every security project that takes profit — from registrars to security vendors to threat intel platforms — they're all limited in what they can say and do. That's the reality of the game.

The Problem With Profit

You know the biggest problem with the security industry?

Those who profit from it are limited. That's reality. There's risk.

What They Can't Do

- They can't call out NameSilo for ignoring abuse reports — even though it's true
- They can't expose Webnic or NiceNic for enabling blood money at scale — too risky
- They can't publish brutal investigations into registrar negligence — lawsuits incoming

- They can't name and shame hosting providers protecting scam infrastructure — business relationships matter
- They can't speak the uncomfortable truth about how broken the abuse system is — partnerships at stake

Is it scary? **Yes.**

Is it the truth? **Absolutely.**

But that's where I come in. I love the harsh, uncomfortable truth. Because scam infrastructure — and especially abuse report negligence — is fucked up.
And *PhishDestroy* , the one that doesn't take profit, can afford to say out loud — without whispering — the truth that inconveniences the world.

What Zero Profit Enables

When you don't take money, something magical happens:

You can't be bought. You can't be threatened. You can't be silenced.

Unfiltered Truth

We can write things as they are. Name registrars enabling scams. Expose hosting providers protecting criminals. Document systematic abuse negligence.

No Conflicts

No sponsors to appease. No partnerships to protect. No revenue streams that could be threatened by telling uncomfortable truths.

Pure Mission

Our only goal is destroying phishing infrastructure. Not growing ARR. Not pleasing investors. Not maintaining business relationships.

Maximum Impact

At any cost to the project's commercial viability. Because there is no commercial viability to protect. We're free to cause maximum damage to scammers.

The Registrar Problem

Let me be specific about one example that perfectly illustrates this:

NameSilo ignores abuse reports. They do. Massively. Systematically. We have the data. We have the emails. We have the ignored reports stacking up while scam domains stay live.

Webnic? Same story. NiceNic? Absolutely.

Do they hate our emails? *Probably.*

Do we hate the scams they're essentially enabling by closing their eyes, not implementing proper abuse handling, ignoring reports, or sending automated responses that mean nothing? **Absolutely.**

But that's why PhishDestroy exists — the psycho project that's changing the game and demanding ethics in an industry that doesn't want to be held accountable.

How It Started (The Real Story)

In the beginning, it was a joke. Seriously.

Started in 2019 as a small Discord crew having fun disrupting Steam phishing rings. It was **trolling at scale** — automated abuse bots destroying thousands of scam domains while scammers lost their minds trying to figure out who was hitting them.

We laughed as they started reporting each other's domains. We watched the chaos multiply without us doing anything.

It was entertainment. It was effective. It was *free* .

Then Something Changed

We realized our work wasn't just destruction — it was helping people.

Our scans ended up as evidence in real investigations. When scammers wiped everything, our archives stayed. URLScan captures we published years ago were being used in court cases. Victims were finding our data and understanding what happened to them.

What started as trolling became something that actually mattered.

The Evolution

So we went harder. Built better systems. Created AI that studies scam patterns. Developed automated reconnaissance. Started playing at a professional level — while staying completely free, independent, and brutally honest.

And you know what? **It works.** The joke became effective. The trolling became professional-grade threat intelligence. The free project became something even governments reference.

Why This Model Works

Here's the asymmetric warfare equation that breaks scammers:

They Invest

Money for domains. Time for infrastructure. Energy defending their operations. Hope for profit.

We Automate

Press a button. Destroy operations. Zero cost. Maximum damage. Repeat infinitely.

They Lose Everything

Domains gone. Infrastructure burned. Money wasted. Mental collapse from fighting an enemy that doesn't care.

We Keep Going

No burn rate. No runway. No investors to answer to. Just pure, sustainable destruction.

They can't comprehend this. They think in terms of profit and loss. They calculate ROI. They assume everyone has a price.

We don't. And that's what destroys them psychologically before we ever touch their infrastructure.

What We Can Do That Others Can't

Because we're outside the profit system, we can:

Say The Quiet Part Out Loud

- Name registrars enabling scams through negligence
- Document systematic abuse of the domain system
- Expose the financial incentives keeping scam infrastructure alive
- Publish investigations others won't touch
- Call out industry complicity without fear of consequences

We write things **as they are** . We call things **by their names** . We don't soften language to protect feelings or business relationships.

Is NameSilo ignoring abuse? *We say it.*

Are registrars profiting from blood money? *We document it.*

Is the abuse reporting system fundamentally broken? *We prove it.*

Truth over comfort. Impact over profit. Ethics over business relationships. Always.

The Personal Motivation

People always want to know the "real" reason. The personal motivation behind spending years on this.

Here it is:

I grew up wealthy. Privileged spaces. Everything on demand. But I saw something that disgusted me — people with money who had the mentality of someone starving. Greedy. Petty. Toxic.

That curiosity led me into the scammer underworld. Into their psychology. Into their broken, hollow existence.

And I understood something fundamental:

They Are Hollow

Scammers don't understand the damage they cause. They don't see destroyed trust, real victims, irreversible harm. Their world is hollow. Their motivations are hollow. **They are hollow.**

And hollow things collapse easily when you apply the right pressure.

So I stayed longer than they expected. Built systems they couldn't comprehend. Created automation that turns their own sloppiness into their downfall.

Not for money. Not for recognition. But because *a world with fewer parasites is simply a better world.*

Why We Stay Free Forever

We get offers. Constantly.

Sponsors wanting to fund us. Companies wanting to acquire our data. Security vendors wanting partnerships. Registrars offering "collaboration opportunities" (read: buying our silence).

We reject them all.

Not out of principle alone — though that matters. But because *the moment we take money, we lose the one weapon that makes us effective: the ability to tell uncomfortable truths.*

The PhishDestroy Promise

We will never take profit from this work.

We will never soften our language to protect business interests.

We will never stop exposing the truth, no matter who it inconveniences.

Because someone needs to be the psycho in the room willing to say what everyone else is too scared to admit.

The Impact You Don't See

Here's what we've actually accomplished by staying free and unfiltered:

Our investigations have been cited in: Government cases. Court proceedings. Academic research. Security industry reports. Mainstream media coverage.

Our data has helped: Victims understand what happened. Investigators build cases. Researchers track new threats. The industry acknowledge problems they'd rather ignore.

Our pressure has forced: Registrars to improve abuse handling (slowly, reluctantly). Hosting providers to terminate accounts. Payment processors to cut off scammers. The ecosystem to be slightly less comfortable with negligence.

None of this would be possible if we were profit-driven. Because profit creates alignment with the status quo. And the status quo protects scammers.

The Real Game We're Playing

While scammers think they're fighting a security project, they're actually fighting something far more dangerous:

An ideology that can't be bought, threatened, or stopped.

We don't need to win every battle. We just need to make their operations unsustainable. Make their infrastructure fragile. Make their profit margins negative. Make their psychological state collapse from fighting an enemy that doesn't even care enough to fight back — we just press buttons and watch their world burn.

The Long Game

Every domain we take down costs them money. Every report we file costs them time. Every investigation we publish costs them credibility. Every tool we build makes the next operation easier.

And it costs us *nothing* .

That's asymmetric warfare. That's why we win.
#AntiPhishing #Values #Mission #Independent #CyberSecurity

See Our Work

Impact Metrics
810,000+ domains tracked, 330,000+ active threats, 99,000+ reports filed.
Anatomy of a Takedown
Step-by-step walkthrough of how we take down phishing infrastructure.
About PhishDestroy
Who we are, what we do, and why we fight phishing.
Tools for Fighting Scams
Community tools and resources to help combat online fraud.
Responsible Disclosure
Our disclosure policy and how we handle vulnerability reports.