

Is dot.ph legit? TrustSniffer's high-trust assessment: 100/100

dot.ph

Verdict

100

OUT OF 100

HIGH TRUST

dot.ph appears legitimate.

Our checks found nothing pointing to fraud. Ordinary care still applies when you pay or sign in.

Not Scam

Safe for Login

Low Risk

Assessed 2026-08-10 by automated analysis. Classification confidence 75%.

What this site appears to be

Official dotPH site offering domain registration and related services for the Philippines (.ph and variants). Provides hosting, SSL, marketplace, pricing, payment options and support contact details. Appears to be an established registry/registrar with transparent product listings.

Evidence status and limitations

- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	26 years old Registered history	CLEAR
Web archive	Archived since 2000 707 snapshots	CLEAR
Certificate	Encrypted connection Issued by Sectigo Public Server Authentication CA DV R36	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Not Scam.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2000.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website presents itself as the official Philippine country-code domain registry and registrar, offering .ph domain registration and related services for businesses and other registrants. Its apparent business model is commercial management of domain names and associated online infrastructure services.

Scam/Impersonation Risk

No contradictions were observed across the supplied evidence: there was no confirmed phishing, impersonation, or malicious-reputation finding. The homepage's stated purpose, service structure, contact options, and domain-registry content are coherent with the apparent dotPH business model. A weak automated resemblance association with another online brand was not corroborated by the site's content and is therefore not treated as an identity contradiction. The website is consequently consistent with an established, apparently legitimate service, although the real-world operator identity remains independently unverified.

EVIDENCE

- The homepage identifies the service as "The Official Domain Name Registry of the Philippines" and provides coherent domain-registration and registrar functions.
- External reputation checks recorded 0 malicious and 0 suspicious detections, with no phishing or impersonation finding.
- The domain was registered in 2000 and is approximately 25.96 years old.
- The archive contains 707 snapshots spanning 2000–2026, covering 27 years of observed history.

Regulatory Verification Notes

The site provides substantive commercial and policy material, including domain registration and renewal, hosting, SSL certificates, marketplace services, WHOIS, FAQs, and Policies, Agreements and UDRP information. It also presents hosting, SSL, Microsoft 365, Google Workspace, and domain-marketplace offerings, indicating a broad registrar and online-services business rather than an investment or brokerage proposition. No specific regulatory licence or registration number is disclosed in the supplied legal and service content; this is a transparency item for confirmation, not evidence of fraud. The available evidence supports an established-site assessment, but it does not independently verify the legal entity operating the service.

EVIDENCE

- The homepage and product areas list .ph, .com.ph, .net.ph, and .org.ph registration, renewal, hosting, SSL, marketplace, and productivity services.
- The About, Contact, FAQ, WHOIS, Policies, Agreements and UDRP areas provide identifiable service and governance content.
- The site is served from AS13335, CLOUDFLARENET – Cloudflare, Inc., US.
- TLS uses the Sectigo Public Server Authentication CA DV R36 issuer, validation level DV, and is valid through 2026-12-18T23:59:59+00:00.

What to Verify Next

Before credential or payment interaction, an interested party should independently confirm the operator's legal identity, compare the applicable domain and hosting terms with the intended transaction, and confirm available payment protection, renewal, cancellation, and dispute provisions. Where a regulated service is required for a particular transaction, the relevant authority's registry should be checked for the responsible entity. Official support channels should also be confirmed through an independently sourced reference rather than relying solely on the website.

EVIDENCE

- The reviewed homepage contains three forms: search, newsletter subscription, and checkout/account creation; no sensitive form or untrusted submission destination was detected.
- The site exposes FAQ, WHOIS, policies, agreements, and UDRP materials that can be used to reconcile service and dispute terms.
- The contact area provides support routes for hosting and domain issues, creating a direct channel for transaction and service confirmation.

Summary Verdict

The overall posture is **high trust and low risk**, and the available evidence is consistent with an established, apparently legitimate website. This conclusion reflects strong convergence among the site's coherent business content, long operating history, clean external reputation, and functioning security infrastructure; it does not constitute independent proof of the operator's real-world identity.

Infrastructure Integrity

The website is protected by Cloudflare CDN/WAF infrastructure, which is a meaningful mitigating control for availability and direct exposure of the service environment but is not, by itself, proof of legitimacy. Observed resolution includes Cloudflare edge servers and potential origin candidates, so infrastructure protection should be treated as layered risk reduction rather than an identity signal.

EVIDENCE

- Cloudflare CDN/WAF protection was observed, with edge IPs 104.20.39.134, 172.66.153.59, 2606:4700:10::6814:2786, and 2606:4700:10::ac42:993b.
- The infrastructure resolved successfully through Cloudflare-operated delivery services.

Closing Assessment

Ordinary browsing and standard service evaluation are proportionate to the assessed posture, while independent merchant-identity, contractual, and payment-protection checks should be completed before credentials or payment details are submitted.

Written analysis generated 2026-08-10 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

No rule findings contributed to this verdict.

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	50%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of dot.ph.

- The request stayed on dot.ph. It was not redirected to another domain. CLEAR
- The earliest public archive of this site is from 2000-08-23. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Not available
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:10::ac42:993b
Name servers	Not available
SSL issuer	Sectigo Public Server Authentication CA DV R36
SSL expiry	2026-12-18
Domain age	25.96 years (continuous registration)
Domain expiry	Not available
Archive first seen	2000-08-23
Archive snapshots	707

Reputation

VirusTotal: 0 flagged | AbuseIPDB: 0 reports | Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about dot.ph at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/dot.ph> · assessed 2026-08-10