

Is plpsupport.com a scam? TrustSniffer's high-risk assessment: 0/100

plpsupport.com

Verdict

0

OUT OF 100

CRITICAL RISK

plpsupport.com shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

A short informational landing page indicating the domain is used for employer-run phishing simulation and security awareness training. No forms or transactions present.

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	10 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	5.0 years old Registered history	CLEAR
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

<https://plpsupport.com/>



What plpsupport.com served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2021.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website is a short informational landing page presenting itself as an employer-managed phishing-simulation and security-awareness training page. It states that the domain is used to teach employees to recognize phishing attacks, does not present a transaction flow, and directs questions to the employer's IT administrator.

Scam/Impersonation Risk

The site's homepage is consistent in content and behavior with a phishing-simulation landing page: it contains explanatory text, no login or sensitive-data form, and no transaction mechanism. However, this benign presentation conflicts with the domain's external threat posture, which includes multiple malicious detections and confirmed blacklist status. The available evidence does not establish that the site is impersonating a named brand or that it is itself conducting credential theft, but the confirmed external detections create a material risk for sensitive interaction and warrant treating the domain as potentially unsafe despite its stated training purpose.

EVIDENCE

- The homepage states that the site is hosted and managed for phishing-simulation purposes and is intended to teach employees how to recognize and avoid phishing attacks.
- The homepage contains no login form, sensitive-data form, payment flow, or external submission destination.
- External reputation telemetry recorded 10 malicious detections and 1 suspicious detection, with a confirmed blacklist status and a Tier-1 threat detection.
- The domain was registered on 2021-08-17 and is recorded as approximately 5.01 years old.

Regulatory Verification Notes

The available page content does not identify a legal entity, licensing authority, registration number, or regulated-service authorization. Given the stated security-awareness purpose, the absence of financial-service claims is relevant, but it does not independently validate the operator's identity; identity verification remains unverified. The technical certificate and hosting records demonstrate operational deployment only and should not be interpreted as evidence of ownership or regulatory standing.

EVIDENCE

- The homepage provides a training-purpose explanation but no identifiable corporate operator or licensing disclosure.
- The site is served from AS35985, identified as ONERINGNET-ATL-1 — One Ring Networks, Inc., US.
- The transport certificate is issued by YE2, uses DV validation, and is valid through 2026-10-21.
- No matching broker signal was identified in the available third-party broker context.

What to Verify Next

Before any credential submission or other sensitive interaction, the purported employer should confirm through an independently known IT or security channel that this exact domain was intentionally deployed for an awareness exercise. Security teams should also preserve the link and associated message for internal review, confirm whether the exercise has been closed, and validate any related communications through established corporate systems rather than the observed domain.

EVIDENCE

- The homepage identifies the intended point of contact as the employer's IT administrator.
- The site's observed purpose is limited to phishing simulation and security-awareness messaging, with no stated commercial transaction process.
- The external reputation record contains a confirmed blacklist status that requires direct organizational confirmation before sensitive use.

Summary Verdict

The overall posture is **critical trust risk** with a high likelihood that sensitive interaction could expose an organization or its personnel to avoidable security consequences. The stated training purpose is plausible and

internally consistent at the page level, but it does not overcome the confirmed adverse external detections or the lack of independently verified operator identity.

Infrastructure Integrity

The site resolves directly to a single likely origin address hosted by One Ring Networks, Inc. in the United States, with no CDN or WAF identified. Its DV TLS certificate provides transport encryption, but this is only a mitigating technical control and offers no assurance that the site or its operator is legitimate.

Closing Assessment

Interaction should remain limited to controlled, read-only analysis unless the employer’s established security function independently confirms the exercise and authorizes any further handling.

Written analysis generated 2026-08-21 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, external reputation.

01 Governance Risk

- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE
- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.
External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	25%

- 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 plpsupport.com.

- The request stayed on plpsupport.com. It was not redirected to another domain. CLEAR
- Registration is published under Key-Systems GmbH. CLEAR
- DNS for this domain is served by topsec.com, across 4 name servers. NOTED
- The registration is paid up to 2027-08-17. NOTED
- The earliest public archive of this site is from 2021-12-21. CLEAR
- It is hosted on ONERINGNET-ATL-1, from a server in US. NOTED

Domain intelligence

Registrar	Key-Systems GmbH
Hosting	ONERINGNET-ATL-1 - One Ring Networks, Inc., US
Country	US
Server IP	64.191.166.205
Name servers	NS1.IE.TOPSEC.COM, NS2.IE.TOPSEC.COM, NS3.CA.TOPSEC.COM, NS4.EU.TOPSEC.COM
SSL issuer	YE2
SSL expiry	2026-10-21
Domain age	5.01 years (continuous registration)
Domain expiry	2027-08-17
Archive first seen	2021-12-21
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 10 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about plpsupport.com 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.