

Is msupdate.net safe? TrustSniffer's moderate-trust assessment: 50/100

msupdate.net

Verdict

50

OUT OF 100

MODERATE TRUST

msupdate.net is moderately trusted.

Most signals looked ordinary, and some evidence was missing. Read the checks below before you pay or hand over personal details.

Sensitive Interaction Risk

Governance Risk

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

What this site appears to be

A short informational page stating the domain is used for phishing simulation and employee training. It advises contacting the employer's IT administrator if there are questions.

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	2 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	14 years old Registered history	CLEAR
Web archive	Archived since 2001 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YE1	NOTED

The page as captured

<https://msupdate.net/>



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

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2001.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

This website is a short, non-monetized phishing-simulation landing page for employee security awareness training. It tells visitors that the domain is hosted and managed for phishing simulations, explains that such sites are used to teach employees to recognize phishing, and directs questions to the employer's IT administrator.

Scam/Impersonation Risk

The site's stated purpose is consistent with an authorized phishing-awareness exercise: the homepage requests no credentials or payment, contains no login form, and presents no detected brand-impersonation indicators. However, this benign page content conflicts with material external threat telemetry, which recorded malicious detections and a confirmed blacklist status supported by two external sources. The external detections therefore create a material risk for sensitive interaction even though the observed page itself is informational and non-transactional; no separate identity contradiction or brand impersonation was identified.

EVIDENCE

- The homepage is titled “Phishing Simulation Landing Page” and states that the domain is used for employee training and phishing awareness.
- External reputation telemetry recorded 2 malicious detections and 1 suspicious detection, with a confirmed blacklist status.
- Historical records show 112 archive snapshots spanning 2001–2025, covering 25 tracked years.

Regulatory Verification Notes

The available content describes an awareness-training function rather than a financial, investment, or other regulated service, and no license claim or regulatory authority is presented. The page does not independently establish the real-world operator behind the domain, so the site's apparent purpose should not be treated as proof of organizational identity. A matched third-party broker-reputation record was not present. The domain is technically established and uses a named commercial registrar, but those administrative and infrastructure facts do not resolve the sensitive-interaction concern created by the external reputation findings.

EVIDENCE

- Domain registration records show creation on 2012-06-19, an age of 14.18 years, expiration on 2027-06-19, and registration through GoDaddy.com, LLC.
- The site is served from AS35985, One Ring Networks, Inc., US.
- The transport certificate is issued by YE1, uses Domain Validation (DV), and is valid through 2026-10-22.

What to Verify Next

Before treating a page encounter as an authorized exercise, the employer or sponsoring organization should confirm the campaign through an independently obtained IT or security-team contact route rather than relying solely on the page. Security teams should also confirm that the domain is included in the organization's approved phishing-simulation inventory and that any associated message was generated through an authorized internal testing process. Login, credential submission, payment, or other sensitive activity should occur only after that independent confirmation.

EVIDENCE

- The homepage specifically directs questions to the employer's IT administrator.
- Two page-behavior runs completed successfully and detected no external network activity, hidden forms, password forms, wallet activity, clipboard activity, or cloaking.
- The captured page contains no payment or credential-collection mechanism.

Summary Verdict

The overall posture is **moderate trust with elevated sensitive-interaction risk**. The site presents a plausible, low-complexity training purpose, but that apparent legitimacy is outweighed for sensitive use by confirmed external threat detections and the absence of independently verified operator identity. The site should therefore be treated as potentially authorized only within a separately confirmed organizational exercise.

Infrastructure Integrity

The site resolves directly to a single likely origin, with no CDN or edge IPs detected. This architecture provides no evident CDN/WAF separation or edge-layer mitigation; infrastructure characteristics should consequently be treated as neutral technical context rather than evidence of legitimacy.

Closing Assessment

Interaction should remain limited to an independently confirmed security-awareness exercise, with sensitive actions deferred until the sponsoring organization verifies the domain through an offline or separately sourced channel.

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.

- 01 Governance Risk

 - The public registration record for this domain is incomplete.
Registration and ownership rule:KF_WHOIS_INCOMPLETE
- 02 Sensitive Interaction Risk

 - The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat

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 msupdate.net.

- The request stayed on msupdate.net. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com, LLC. CLEAR
- DNS for this domain is served by intelliwire.net, across 3 name servers. NOTED
- The registration is paid up to 2027-06-19. NOTED
- The earliest public archive of this site is from 2001-07-03. CLEAR
- It is hosted on ONERINGNET-ATL-1, from a server in US. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	ONERINGNET-ATL-1 - One Ring Networks, Inc., US
Country	US
Server IP	64.191.166.198
Name servers	NS1.INTELLIWIRE.NET, NS2.INTELLIWIRE.NET, NS3.INTELLIWIRE.COM
SSL issuer	YE1
SSL expiry	2026-10-22
Domain age	14.18 years (continuous registration)
Domain expiry	2027-06-19
Archive first seen	2001-07-03
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 2 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about msupdate.net 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/msupdate.net> · assessed 2026-08-21