

Is Office-365.co.uk a scam? TrustSniffer's high-risk assessment: 0/100

Office-365.co.uk

Verdict

0

OUT OF 100

CRITICAL RISK

Office-365.co.uk 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 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

A short landing page explicitly labelled as a phishing domain used for employee security training. Contains brief explanatory text and contact prompt; no forms or transactional elements 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.

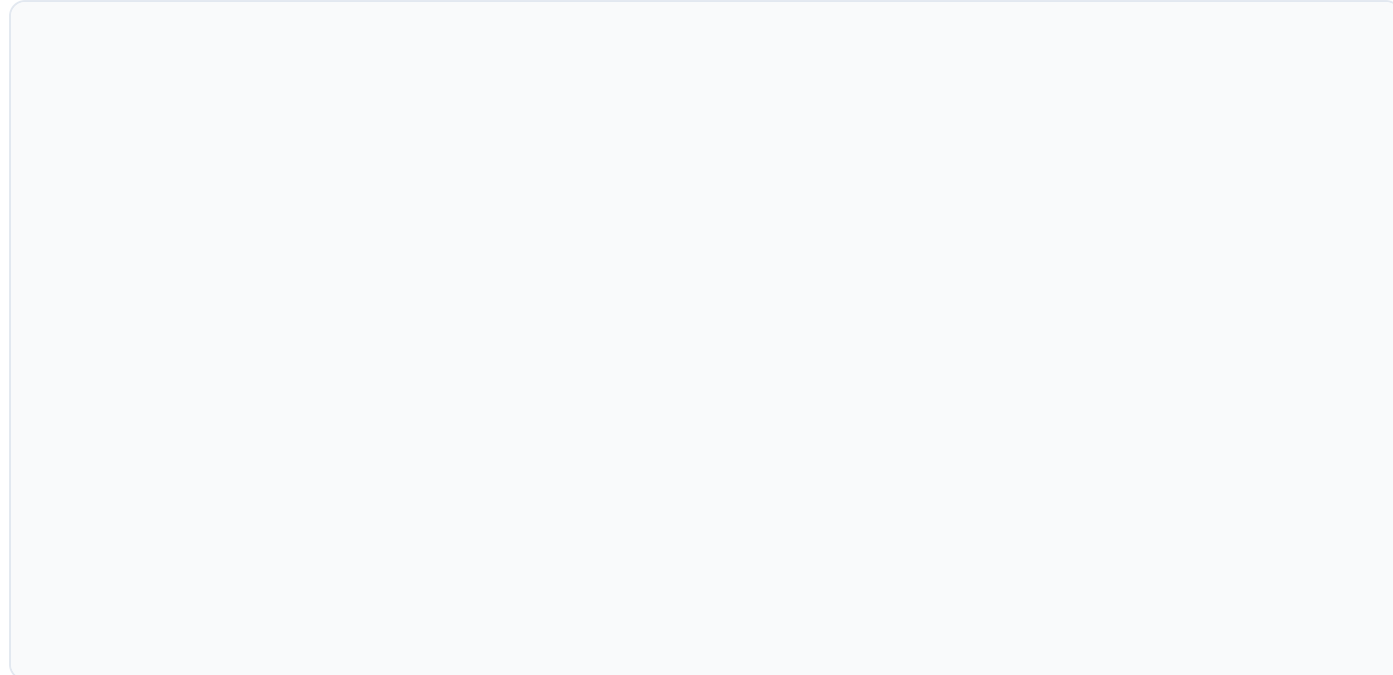
At a glance

The checks that decide most of this verdict.

Malware engines	14 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	5.1 years old Registered history	CLEAR
Web archive	Archived since 2021 10 snapshots	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://office-365.co.uk/en>



What Office-365.co.uk served when TrustSniffer captured it on 2026-08-18. 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

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

The website is a short security-awareness landing page presented as a phishing-training domain. It tells visitors that they have reached one of “Phished’s” domains, explains that such domains are used to educate and train enrolled employees, and provides a contact prompt rather than offering products, transactions, or credential-collection forms.

Scam/Impersonation Risk

The site has a **critical security posture** because external threat intelligence recorded a confirmed blacklist condition and multiple malicious detections, including detections from major security providers. These signals are materially stronger than the page-level presentation, which appears informational and does not itself collect credentials or solicit funds. No conflicting legal-entity names or direct brand-impersonation finding were identified, but the confirmed blacklist status is sufficient to create a serious contradiction for sensitive interaction. The site’s explicit description as a phishing-training domain may explain the security detections, but it does not make the domain appropriate for authentication or other sensitive activity without independent authorization.

EVIDENCE

- External reputation assessment recorded 14 malicious detections from 19 evaluated results and a confirmed blacklist condition across two external sources.
- Domain registration records show registration on 2021-07-28, with an age of 5.06 years, through OVH.
- Archive records show 10 snapshots spanning 2021-11-23 through 2025-03-08, covering 5 tracked years.
- The homepage states: "You've ended up on one of our phishing domains!" and describes employee-training use, while presenting no login or sensitive form.

Regulatory Verification Notes

The available page is informational rather than a financial or transactional service, and it makes no licensing or regulated-entity claim. However, the visible content does not establish a legal operator, corporate identity, or authorization relationship for the training activity; the operator identity therefore remains unverified. This is a verification and disclosure gap rather than, by itself, proof of fraud. A separate broker-reputation check produced no match, but that contextual result does not establish licensing or legitimacy. The valid certificate confirms encrypted transport only and does not authenticate the operator.

EVIDENCE

- The hosting infrastructure is identified as AS13335, CLOUDFLARENET – Cloudflare, Inc., US.
- The site uses a DV TLS certificate issued by WE1, valid to 2026-09-21.
- The visible landing page contains a brief training explanation and contact prompt but no legal-entity, licensing, or registration disclosure.

What to Verify Next

Before any access beyond passive review, the purported sponsoring organization should confirm through an independently sourced or offline channel that this domain is an authorized component of its employee-training program. Security teams should also check the domain against internal email, web-proxy, and endpoint controls before allowing access, and should preserve the original referral or training notification for comparison. No authentication, credential submission, payment activity, or other sensitive interaction should occur unless that authorization is independently confirmed.

EVIDENCE

- The site provides only a generic contact prompt as its stated visitor follow-up route.
- The page contains no login form, hidden sensitive form, or transaction mechanism.
- The available content identifies a training scenario but does not independently document the customer or organization authorizing it.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The apparent informational purpose is not sufficient to offset the converging external threat signals and the absence of independently verified operator identity. The site should be treated as untrusted for account access, credential handling, or financial activity.

Infrastructure Integrity

Cloudflare CDN and WAF protection provide a mitigating layer for traffic delivery and exposure, with observed traffic terminating at the Cloudflare edge rather than an independently visible origin. This infrastructure can improve resilience and reduce direct origin exposure, but it is a shared protective service and does not establish that the website itself is legitimate.

Closing Assessment

The domain should remain restricted from sensitive use unless the claimed training relationship is confirmed through an independently sourced channel and the organization’s security controls authorize access.

Written analysis generated 2026-08-18 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, behaviour in a sandbox, external reputation.

- 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
 - Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
 - The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
 - 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	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 Office-365.co.uk.

- The request stayed on Office-365.co.uk. It was not redirected to another domain. CLEAR
- Registration is published under OVH. CLEAR
- DNS for this domain is served by com., across 2 name servers. NOTED
- The registration is paid up to 2027-07-28. NOTED
- The earliest public archive of this site is from 2021-11-23. CLEAR
- It is hosted on CLOUDFLARENET, from a server in BE. NOTED

Domain intelligence

Registrar	OVH
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	BE
Server IP	188.95.12.254
Name servers	david.ns.cloudflare.com., melissa.ns.cloudflare.com.
SSL issuer	WE1
SSL expiry	2026-09-21
Domain age	5.06 years (continuous registration)
Domain expiry	2027-07-28
Archive first seen	2021-11-23
Archive snapshots	10
Reputation	VirusTotal: 14 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about Office-365.co.uk 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/0ffice-365.co.uk> · assessed 2026-08-18