VALIDATION REPORT

CASE STUDY #007

ENTITY CATEGORY:

Digital Infrastructure / SaaS Email Phishing

SUBMISSION TYPE:

Inbound Phishing Email — Zoho Impersonation

This document is a formal record of a VASD three-layer trust assessment conducted against a phishing entity that delivered fraudulent correspondence impersonating Zoho Corporation's billing department. The findings are the result of signal-based analysis across domain intelligence, entity presence, and technical pattern verification. This report is cleared for full public distribution.

DATE	ANALYST	SYSTEM	VERDICT
JUNE 2026	VELURYN AGNECY	VASD v1.0	**HIGH RISK**

CASE STUDY #007 // PUBLIC // Zoho Billing Impersonation — One-Day Domain Phishing Attack

SECTION 00

OPENING STATEMENT

Every entity that reaches into someone's inbox is making a claim. A claim about who they are, what they represent, and why they deserve a response. Most people accept that claim at face value. They should not.

VASD was built for one purpose: to interrogate that claim before anyone acts on it. Not with suspicion as a default. With method. With structure. With layers.

This session was initiated upon receiving correspondence purporting to originate from Zoho Corporation's billing department. The entity claimed a failed payment against an active subscription and directed the recipient to update payment credentials via an embedded link. VASD examined each element of that claim independently.

> "*The core of the reactor was not destroyed by the explosion. It was destroyed by what happened before the explosion — the decisions, the assumptions, the things that were never checked.*"
>
> — Format of thought that guides this report.

SYSTEM STRUCTURE

HOW VASD WORKS

VASD does not make a decision after one observation. It builds a case. Three layers. Each one narrower, deeper, and harder to deceive than the last.

LAYER 1

Initial Screening. Domain age. Provider type. Message consistency. Surface-level red flags.

LAYER 2

Real-World Presence. Website, social footprint, brand consistency, public records.

LAYER 3

Deep Verification. Cross-check all claims. Historical signals. Hidden inconsistencies.

SECTION 01

LAYER 1 — INITIAL SCREENING

The first layer asks: does anything here fail immediately? This entity failed on first contact. The sender domain had no verifiable connection to Zoho Corporation. The first layer did not need to proceed far before critical indicators surfaced.

SIGNAL	FINDING	STATUS
Sender Domain	customer-notifications.com — not affiliated with zoho.com or zohocorp.com. Zoho's legitimate billing emails originate exclusively from @zoho.com.	× HIGH RISK
Domain Age	Registered 2026-06-18 — one day before email delivery on 2026-06-19. Single-year registration. Status: client transfer prohibited. Classic throwaway domain pattern.	× HIGH RISK
Email Provider Type	Custom domain used. However, the domain has no verifiable connection to any legitimate corporate entity. Custom domain alone does not confer legitimacy.	■ FLAGGED
Redirect Mechanism	UPDATE BILLING button routes through a rebrand.ly short-link. True destination URL deliberately obfuscated. Legitimate Zoho billing links resolve directly to accounts.zoho.com.	× HIGH RISK
Spam Filter Signal	Zoho's own mail infrastructure flagged the email at delivery: "Email content matches the prevalent spam patterns." System-level red flag confirmed on receipt.	■ FLAGGED
Message Tone	Urgency-engineered language throughout. "Second failed payment," "service disruption" threat, red CTA button. Manufactured pressure pattern applied systematically.	■ FLAGGED

LAYER 01 VERDICT — INITIAL SCREENING

HIGH RISK — 3 critical indicators, 3 flags. Layer 1 alone is sufficient to confirm this entity as a threat.

The domain was registered 24 hours before use. The sender address is a fabricated lookalike. The redirect chain deliberately conceals the destination. These are not ambiguous signals — they are the architecture of a phishing campaign.

SECTION 02

LAYER 2 — REAL-WORLD PRESENCE

The second layer does not ask whether the entity looks real. It asks whether the entity is real. In this case, the entity behind the phishing infrastructure has no verifiable real-world presence whatsoever. This layer is documented in full to confirm the total absence of legitimate footprint.

SIGNAL	FINDING	STATUS
Sender Entity	No company named "Zoho Billing" or operating from customer-notifications.com exists in any publicly accessible business registry.	× HIGH RISK
Primary Website	customer-notifications.com has no public-facing website. The domain resolves to email infrastructure only. No company identity, address, or contact information published.	× HIGH RISK
Physical Address	No verifiable physical address associated with the sending domain or its registrant. Registrant information is privacy-shielded via Cloudflare.	× HIGH RISK
LinkedIn Presence	No LinkedIn company page, social media profile, or online footprint associated with the domain or any entity operating from it.	× HIGH RISK
Third-Party Records	Domain flagged in zero third-party trust databases as a legitimate business entity. No review history, no business directory listing, no public record of operations.	× HIGH RISK
Visual Impersonation	Email replicates both the Zoho Workplace logo and the ZOHO colour-block signature. Both are copied assets. Their presence does not indicate affiliation with Zoho Corporation.	■ FLAGGED

LAYER 02 VERDICT — REAL-WORLD PRESENCE

HIGH RISK — Entity has no verifiable real-world presence across any independent source.

No website. No address. No social presence. No business registration. The only thing this entity has is a one-day-old domain and copied logos. That is not a company. That is infrastructure built for a single attack.

SECTION 03

LAYER 3 — DEEP VERIFICATION

The third layer is where the careful deceptions surface. By Layer 3 this entity had already failed on every prior signal. What this layer documents is the technical architecture behind the attack — the infrastructure choices that confirm intent, not accident.

SIGNAL	FINDING	STATUS
Registration-to-Attack Timing	Domain customer-notifications.com registered 2026-06-18. Email delivered 2026-06-19. A 24-hour gap between domain creation and deployment is a confirmed phishing pattern. No legitimate business registers a domain and sends billing emails the next day.	× HIGH RISK
URL Redirect Chain	UPDATE BILLING routes through rebrand.ly — a legitimate URL shortener being weaponised as a trust proxy. The final destination could not be safely resolved. This two-step redirect architecture is designed to evade link-scanning security tools.	× HIGH RISK
Domain Infrastructure	Cloudflare nameservers used (eva.ns + jim.ns.cloudflare.com). Cloudflare's free tier masks the true hosting origin. Combined with a fresh creation date and single-year registration, this is consistent with infrastructure built solely for a one-time phishing operation.	× HIGH RISK
Urgency Engineering Pattern	Three-layer pressure stack applied: (1) "second failed payment" — implies prior warning, (2) "service disruption" threat — financial consequence framing, (3) red CTA button — visual alarm signal. This is a documented social engineering sequence.	× HIGH RISK
Grammar and Copy Anomalies	"Being charges for services rendered to at you request" — grammatically malformed. Inconsistent with Zoho Corporation's editorial standard. Indicative of machine-generated or rushed non-native copy.	■ FLAGGED
Spam Compliance Mimicry	A functional unsubscribe link is present. Phishing operators deliberately include CAN-SPAM/GDPR compliance markers to pass heuristic spam filters that check for their absence. It signals awareness of detection systems, not legitimacy.	■ FLAGGED

LAYER 03 VERDICT DEEP VERIFICATION

HIGH RISK — 4 critical indicators, 2 flags. All technical signals confirm coordinated phishing infrastructure.

The registration timing alone is a disqualifying signal. Every subsequent finding compounds it. This is not an ambiguous case. This is a documented, deliberate attack.

SECTION 04

FINAL JUDGMENT

VERDICT: HIGH RISK

This entity is not a real organisation. It is infrastructure assembled for a single fraudulent operation. It has no physical presence, no operational history, no employee footprint, and no legitimate affiliation with Zoho Corporation or any of its subsidiaries.

The domain customer-notifications.com was registered 24 hours before the phishing email was delivered. The billing CTA routes through a URL shortener to conceal the destination. The email copy was urgency-engineered with a three-layer pressure sequence. Zoho's own spam infrastructure flagged the message. Every observable signal confirms deliberate, coordinated deception.

The presence of Zoho branding assets within the email does not indicate affiliation. Logos are public. Colour schemes are replicable. What cannot be replicated is a legitimate domain, a real corporate address, a verifiable business registry entry, or a customer relationship that predates the attack.

RECOMMENDATION: Do not click any link in this email. Do not enter payment or card details on any page reached via this email. Report the sender domain to Zoho Security (abuse@zoho.com) and your email provider. If payment details were entered prior to this assessment, contact your bank immediately and request card cancellation.

LAYER SUMMARY

LAYER	NAME	FLAGS	RESULT
01	Initial Screening	6	HIGH RISK
02	Real-World Presence	6	HIGH RISK
03	Deep Verification	6	HIGH RISK
FINAL	**Combined Judgment**	**18**	**HIGH RISK**

This report was produced by VELURYN AGNECY — VASD Division. For inquiries: vivin.b@velurynagnecy.com