

Actual mail text

From alert@amazon-support.com

Subject: Your Amazon Account is Locked-Immediate Action Required

Dear Customer,

We noticed unusual activity in your Amazon account. For your protection, we have temporarily locked your account

To unlock your account, please verify your identity by clicking the link below,

<https://amazon.verify-account-secure.com>

If you do not respond within 24 hours, your account will be permanently suspended.

Thank you for being a valued customer,

Amazon Support Team

Attachment: Amazon Verification Form.cocm

Phishing Email Analysis

Email Overview

- Subject: Your Amazon Account is Locked Immediate Action Required
- From (Displayed): Amazon Support <alert@amazon-support.com>
- Body Content:

We noticed unusual activity in your Amazon account. For your protection, we tuve temporarily locked your account. To unlock your account, please verify your kenlity by clicking the link below

<https://amazon.verify-account-secure.com>

If you do not respond within 24 hours, your account will be permanently Suspended

- Phishing Indicators (Email Body)

Indicator

Description

Spoofed Email Address amaz0n-support.com looks similar to amazon.com, but includes a zero (0) instead of an "o".

Suspicious URL Link displayed as "amazon" but points to verify-account-secure.com, a non-Amazon domain.

Urgent Language Uses pressure tactics: "Immediate Action Required", "Account Locked", "Respond within 24 hours".

Attachment Type .docm file extension can contain malicious macros.

Generic Greeting Uses "Dear Customer" instead of the recipient's name.





Grammar & Tone Slightly awkward phrasing designed to trigger a panic response.

Email Header Analysis

Header Snippet (Simulated):

Return-Path: <alert@amaz0n-support.com>
Received: from mail.fakehosting.ru (185.244.25.92)
Authentication-Results: dkim=fail; spf=fail; dmarc=fail

Key Findings:

Header	CheckResult	Explanation
SPF	 Fail	The sending server (IP: 185.244.25.92) is not authorized to send on behalf of amaz0n-support.com.
DKIM	 Fail	The email's DKIM signature could not be verified — common in spoofed emails.
DMARC	 Fail	Fails to meet domain policy checks.
Return Path Mismatch	 True	Return path differs from actual sending server, which is a red flag.
Origin Server IP	185.244.25.92	This IP is not owned by Amazon, and may belong to a known spam host.

Tools Used

- MxToolbox Email Header Analyzer

- Email client to view full message source
- Browser to hover and inspect URLs

Conclusion

This email is a clear **phishing attempt** that uses:

- ☐ A spoofed domain
- ☐ Social engineering techniques (urgency & fear)
- ☐ Malicious attachment
- ☐ And technical red flags from header analysis

The email fails SPF, DKIM, and DMARC checks and comes from a suspicious IP address. The user is advised not to click any links or open attachments and to report the email immediately.