Phishing Email Analysis Report

Sample Phishing Email

From: support@amaz0n-customerservice.com

Subject: Urgent: Your Amazon Account Has Been Locked

Date: May 26, 2025

Dear Customer,

We noticed suspicious activity in your Amazon account. Your account has been temporarily locked for your security.

Please verify your information immediately by clicking the link below:

[Click here to verify](http://amazon-security-check.com/login)

Failure to act within 24 hours will result in permanent suspension of your account.

Thank you,

Amazon Security Team

1. Sender Email Address Analysis

Email used: support@amaz0n-customerservice.com

Suspicious Pattern:

- Domain is not official (amaz0n instead of amazon - a common typosquatting trick).

- Subdomain-style email (customerservice.com) adds to the impersonation.

2. Header Analysis

Used a free tool: https://mxtoolbox.com/EmailHeaders.aspx

Findings:

- SPF/DKIM checks failed or not present.

- "Received" IP does not match Amazon mail servers.

- Discrepancy between the "From" and "Return-Path" addresses.

3. Suspicious Links

Hovered link: http://amazon-security-check.com/login

Red flags:

- Domain is not related to Amazon.

- Plain HTTP instead of HTTPS.

- Likely phishing site designed to steal login credentials.

4. Urgent or Threatening Language

Examples:

- "Urgent: Your Amazon Account Has Been Locked"

- "Failure to act within 24 hours will result in permanent suspension"

Tactic: Induces panic to force immediate action.

5. Spelling/Grammar Errors

Not many errors, but some minor unnatural phrasing like "Failure to act..." and "has been temporarily locked for your security."

6. Brand Impersonation

Claims to be from Amazon but no official logo, formatting, or verified domain.

Uses psychological tricks (urgency, fear) common in phishing.

Summary of Phishing Indicators

Indicator	Description
Spoofed email address	amaz0n-customerservice.com is not a valid Amazon domain
Mismatched URLs	Link appears legitimate but points to fake domain
Urgent and threatening language	Pressure tactics to rush the user
Header discrepancies	Fails authentication checks (SPF, DKIM), IP mismatch
Lack of professionalism	Slightly unnatural phrasing, no branding or digital signature
No personalization	Uses "Dear Customer" instead of your real name

Tools Used

- Email header analyzer: https://mxtoolbox.com/EmailHeaders.aspx

- URL Checkers: https://www.virustotal.com, https://www.phishtank.com