Phishing Email Analysis Report

1. Sample Email Content (Obtained)

From: Amazon Support <account-security@amaz0n-billing.com>
Subject: Urgent: Your Amazon Account Has Been Locked
Body:

Dear Customer,

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

To restore access, please verify your identity immediately by clicking the secure link below:

🔗 Verify Now

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

Thank you for your attention,
Amazon Customer Protection

Attachment: Amazon_Account_Report.zip

2. Sender's Email Address – Spoof Check

Suspicious:

- Email address: account-security@amaz0n-billing.com
- Spoofing Attempt: Uses a lookalike domain (amaz0n with a zero) instead of amazon.com.

3. Email Header Discrepancies (From Header Analysis)

Header Flags Found (via analyzer):

- SPF: fail – Sender IP not authorized to send emails for the domain
- DKIM: fail – Digital signature verification failed

- DMARC: fail – Domain policy not satisfied

- Return-Path shows a Russian domain: phisher@compromised-mail.ru
  Conclusion: Email authentication completely fails.

4. Suspicious Links or Attachments

- Attachment: Amazon_Account_Report.zip — Executable attachments in ZIP format are common malware vectors.

- Link (hidden behind “Verify Now”) — URL is hidden, possibly redirecting to a fake login or phishing site.

5. Urgent or Threatening Language

Yes — phrases like:

- "Urgent: Your Amazon Account Has Been Locked"

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

These are common social engineering tactics to pressure the user into acting quickly.

6. Mismatched or Masked URLs

Although the actual destination URL is not shown in the email body, phishing emails typically use a hyperlinked button ("Verify Now") to disguise malicious links. Hovering over the link would likely reveal a mismatched domain.

7. Spelling or Grammar Errors

- The email text itself appears mostly grammatically correct, but the "Amazon Customer Protection" sign-off is not a legitimate department name, indicating inauthenticity.

8. Phishing Traits Found

- Spoofed Email: The sender address amaz0n-billing.com mimics the legitimate domain amazon.com using a zero (0) instead of the letter "o" — a classic example of a lookalike domain used in phishing.

- Header Failures: Email authentication checks failed — SPF, DKIM, and DMARC did not validate the message, indicating it likely did not come from a trusted source.
-
- Threat Language: The email uses urgency and fear tactics like “account locked” and “permanent suspension within 24 hours” to pressure the recipient into immediate action.

- Suspicious Attachment: The .zip file named Amazon_Account_Report.zip is highly suspicious, as compressed attachments are often used to deliver malware.

- Fake Branding: The sign-off uses “Amazon Customer Protection,” which is not an actual department of Amazon, reducing the credibility of the message.

- Hidden Link: The “🔗 Verify Now” link hides the real destination URL, which is a common trick used to redirect users to malicious or fake login pages.

- Slight Authenticity: While the grammar and formatting are relatively clean, this is a tactic used by more sophisticated phishing emails to gain trust and bypass suspicion.