Phishing Indicators Report

Objective:
To analyze a suspicious email and identify characteristics commonly associated with phishing attempts using free tools and manual inspection.

Email Sample Summary

- **Subject:** Urgent: Your Account Will Be Locked!
- **Sender Email Address:** security-update@amazn-alert.com
- **Date Received:** May 25, 2025
- **Attachment(s):** Account_Update_Form.pdf
- **Email Client:** Outlook Web App (OWA)

---

1. Sender Email Address Analysis

- **Observation:** The sender's domain is amazn-alert.com, which is not associated with the legitimate Amazon domain (amazon.com).
- **Phishing Indicator:**
    - Domain misspelling (typosquatting) intended to deceive recipients into thinking it's from Amazon.
    - Use of hyphenated and non-standard domain names often correlates with phishing.
    - This technique is used to bypass naive domain filters and trick users who scan emails quickly.

---

2. Email Header Analysis

- **Tool Used:** MXToolbox Header Analyzer / Google Admin Toolbox
- **Key Header Findings:**
    - **SPF (Sender Policy Framework): Fail**
        - The sender domain’s SPF record does not authorize the sending IP.
    - **DKIM (DomainKeys Identified Mail): Not signed**
        - The message was not cryptographically signed with DKIM, raising authenticity concerns.
    - **Received From IP:** 176.223.133.29 (hosted in Eastern Europe by an unknown VPS provider)

    - **Reply-To Address:** support@unknown-domain.ru, different from the “From” address.

- **Phishing Indicators:**
    - Failed SPF check indicates possible spoofing.
    - No DKIM signature – reduces email authenticity.
    - Mismatched Reply-To domain – common tactic to redirect responses to attacker.
    - Hosting origin from suspicious region, unrelated to sender domain.

---

3. URL and Hyperlink Analysis

- **Link Displayed:** “Click here to verify your account”
- **Actual Link:** http://secure-amazon-login.xyz/verify
- **Method:** Hovered over link to reveal URL.
- **Phishing Indicators:**
    - Displayed text and actual URL do not match.
    - URL uses a deceptive domain (secure-amazon-login.xyz), attempting to mimic Amazon.
    - Usage of HTTP instead of HTTPS – insecure and suspicious.
    - Suspicious TLD (.xyz) commonly used in malicious domains.

---

4. Language and Psychological Tactics

- **Email Excerpt:**
  “We detected unauthorized access to your account. If you don’t confirm your identity within 24 hours, your Amazon account will be permanently suspended.”
- **Phishing Indicators:**
    - Use of **urgency and fear** to prompt immediate action without scrutiny.
    - Common social engineering tactic used to bypass user judgment.

---

5. Spelling and Grammar Errors

- **Examples Identified:**
    - “Your acount need verifycation immediately.”
    - “Click hear to proced to secure page.”
- **Phishing Indicators:**

- Repeated spelling and grammatical errors reflect lack of professionalism.
- Legitimate companies typically review customer-facing communications thoroughly.

---

6. Attachment Analysis

- **File Name:** Account_Update_Form.pdf
- **Inspection Result:**
  - The PDF requests personal information including:
    - Full Name
    - Address
    - Date of Birth
    - Credit Card Number
    - Social Security Number
  - **Phishing Indicators:**
    - Legitimate companies never ask for sensitive information via downloadable forms.
    - This could also potentially be a **malicious payload** containing exploit scripts or data exfiltration code.

---

7. Additional Red Flags

- **No personal salutation** – generic greeting: “Dear customer”
- **Lack of official branding** – low-resolution logo, off-brand fonts
- **No digital signature** – missing common security features like message authentication codes or company-specific footer.

Final Assessment and Conclusion

Based on the comprehensive analysis, the email contains numerous strong indicators of a phishing attempt, including:

- Spoofed and deceptive sender address
- SPF authentication failure
- Mismatched and suspicious URLs
- Use of threatening and urgent language
- Obvious grammar/spelling issues

- A fraudulent attachment soliciting sensitive data
- Overall lack of professionalism and branding

Threat Level: HIGH

Action Recommended: Do NOT open any attachments or click any links. Report to your organization's cybersecurity team or email provider. Block the sender domain and related IP addresses.

Tools Used

- MXToolbox Email Header Analyzer: https://mxtoolbox.com/EmailHeaders.aspx
- Google Admin Toolbox (Messageheader): https://toolbox.googleapps.com/apps/messageheader/
- VirusTotal URL Scanner: https://www.virustotal.com
- PhishTank Verification: https://www.phishtank.com/