🛡️ Phishing Email Analysis Report – Amazon Spoof

**OVERVIEW**

This report documents the analysis of a phishing email impersonating Amazon. The email was crafted to deceive the recipient into clicking a malicious link and opening a harmful `.zip` attachment under the guise of account verification. The purpose is to demonstrate common phishing tactics and how to analyze such emails effectively.

**📧 1. Email Overview**

- Subject: Urgent Action Required – Account Suspended

- From Address: support@amaz0n-service.com

- To: user@example.com

- Attachment: restore\_account\_form.zip

Date Received: [Insert Date]

This email falsely claims to be from Amazon’s support team. It attempts to scare the recipient into restoring access to their account by clicking on a link or downloading an attachment.

**🧾 2. Header Analysis**

The header was analyzed using MxToolbox.  
- SPF: Failed  
- DKIM: Failed  
- DMARC: Failed  
- IP Address: 198.51.100.12 — does not belong to Amazon mail servers  
  
These failures strongly indicate spoofing and unauthorized email sending.

**🌐 3. Sender Domain Analysis**

- Claimed Address: support@amaz0n-service.com  
- Legitimate Domain: amazon.com

Red Flags:  
- Misspelling with a zero (0) instead of 'o'  
- Use of '-service' to mimic official branding  
  
This is a classic case of typosquatting to impersonate a trusted company.

**🔗 4. Link Analysis**

- Visible Link: https://www.amazon.com.account-verify-login.securepage.co/restore  
- Actual Domain: securepage.co → not affiliated with Amazon  
  
VirusTotal Result:  
The link was submitted and flagged by several AV engines as phishing/malicious.  
Appears legitimate at first glance due to subdomain trickery (amazon.com.account-verify...).

**📎 5. Attachment Analysis**

- File Name: restore\_account\_form.zip  
- Content: Contains executable (simulated malware)  
- Scan Result: Identified as potentially harmful via VirusTotal  
  
Zip files are often used to bypass email filters and hide payloads like trojans, stealers, or ransomware.

**🗣️ 6. Language and Tone Analysis**

The email uses:  
- Threat-based language: “Your account will be permanently closed.”  
- Urgency triggers: “Limited your account access.”  
- Generic greeting: “Dear Customer”  
  
Even though grammar appears correct, the tone is manipulative — a hallmark of social engineering attacks.

**🚨 7. Phishing Indicators Summary**

| Indicator | Detected |  
|--------------------------------|----------|  
| Misspelled sender domain | ✅ |  
| Fake URL with legit subdomain | ✅ |  
| Urgent language | ✅ |  
| Unexpected attachment | ✅ |  
| SPF/DKIM/DMARC failures | ✅ |

**✅ 8. Conclusion**

This email is a clear phishing attempt aiming to:  
- Trick the user into submitting credentials on a fake site  
- Deliver a potentially malicious .zip attachment  
- Bypass security controls through domain spoofing and urgency

**🛡️ 9. Recommendations**

- Do not click on any links or open attachments from suspicious emails  
- Educate users on phishing red flags and impersonation tactics  
- Implement SPF, DKIM, and DMARC enforcement  
- Use advanced email filtering tools that can flag spoofed and suspicious content  
- Report phishing to your IT or security team immediately