Phishing Incident — SOC L1 Report

Observed: $(date -R)
Analyst: pintu sharma (lab)

Summary

A simulated phishing email impersonating "Amazon Support" was analyzed for SOC L1 practice. This repository (`phish-lab`) demonstrates safe EML parsing, IOC extraction, and containment steps for SOC L1/Tier-2 training.

Indicators

- **From:** support@amaz0n.com
- **To:** user@victim.local
- **Subject:** Urgent: Verify your account
- **Message-ID:** 12345@amaz0n.com
- **URL:** http://amaz0n-secure-login.xyz/login
- **IP:** 203.0.113.45
- **EML SHA256:** c055ccf9e274557d2adb57be4a09852b6cad946104900e050c7f2d7332086c76

Actions Taken

1. Saved EML and IOCs to secured evidence path (redacted for public).
2. Extracted URLs, headers and attachment hash using `scripts/parse_eml.py`.
3. Examined attachment content (no macros found).
4. Added Postfix test block rules for sender/domain in lab.
5. Generated this report and uploaded to repo `docs/`.

Recommendations

- Block domain/sender at production MX/gateway.
- Search mail logs for similar Message-IDs and quarantine hits.

- Educate users about suspicious “verify account” emails.
- Escalate to IR if credentials were submitted.

Evidence & Artifacts

- Sample EML: `samples/simulated.eml`
- Parser script: `scripts/parse_eml.py`
- Attachment hash: `invoice.docx` SHA256 (sample) in project.

Notes

All samples are simulated and redacted for public sharing. Do NOT include sensitive attachments or PII in public repos; keep raw evidence in a secure internal store.