Simulated Phishing Analysis Report

Analyst: Chandana Devarakonda Date: 2025-09-24

1) Executive summary

This is a simulated phishing email created for training and reporting. The message impersonates 'HackingFlix' and advertises a limited-time course offer. Technical header analysis (simulated) shows SPF/DKIM/DMARC deficiencies and sender-domain mismatches consistent with spoofing. The email contains a tracked link and a zipped executable attachment — high risk for credential theft and malware.

2) Simulated raw headers (excerpt)

Return-Path: Received: from mail-relay-3.hackingflix-offers.com (unknown [203.0.113.45]) by mx.google.com with ESMTPS id r123si0xxxqkj.2025.08.28.09.04.22 From: "Gautam Kumawat" Reply-To: Subject: ■ You got $500, Chandana Devarakonda Authentication-Results: mx.google.com; spf=neutral; dkim=none; dmarc=fail

3) Simulated email body (excerpt)

Hey Chandana Devarakonda, Good News Alert! I got so many emails yesterday that my email account got hanged... (truncated) Link: http://promo.hackingflix-discounts.com/track?uid=Zk1a2b Attachment: invoice.zip (contains setup.exe)

4) Technical findings

- From header mismatch: support@hackingflix.co vs bounce@hackingflix-offers.com vs reply@offers-hftrack.com - SPF=neutral, DKIM=none, DMARC=fail (simulated) - Originating IPs (simulated): 203.0.113.45, 198.51.100.12 - Tracked/mismatched URL: promo.hackingflix-discounts.com - Attachment: invoice.zip -> setup.exe (malware risk)

5) Indicators of Compromise (IOCs)

- Domains: hackingflix-offers.com; hackingflix-discounts.com; offers-hftrack.com - URLs: http://promo.hackingflix-discounts.com/track?uid=Zk1a2b - Attachment filenames: invoice.zip -> setup.exe - Message-ID: <20250828.9F1A23C4@mail-relay-3.hackingflix-offers.com>

6) Risk assessment

Likely objective: credential harvesting and/or malware installation. Severity: HIGH Confidence: HIGH

7) Recommended actions

1. Do not click links or open attachments. 2. Block sender domains/IPs and add IOCs to the mail gateway and EDR blocklists. 3. Quarantine the message and submit attachments to an isolated sandbox for detonation. 4. Notify users and require password resets + enable MFA if compromise suspected. 5. If a device opened the attachment: isolate, image, and perform forensic/malware analysis.

8) Evidence & notes

This is a simulated example for training. Replace simulated IOCs with actual values when analyzing a real sample. Commands used (safe, read-only examples): - sed -n '1,120p' sample-email.eml - egrep -i '^received:|^return-path:|^message-id:|^from:|^reply-to:|^authentication-results:' sample-email.eml - grep -Eo '(http|https)://[^"'" >]+' sample-email.eml | sort -u - file invoice.zip; unzip -l invoice.zip; sha256sum invoice.zip setup.exe