Phishing Email Analysis — Final Report

Trainee: Tarun Arulraj Contact: tarunarulraj23@gmail.com Date: 15 Nov 2025

Phishing Email Analysis — Final Report -------------------------------------

Trainee: Tarun Arulraj Contact: tarunarulraj23@gmail.com Sample ID: sample1 (Flipkart impersonation) Date: 15 Nov 2025

1. Executive Summary This report analyzes a phishing email sample impersonating Flipkart and requesting immediate payment verification. Multiple indicators (authentication failures, mismatched links, insecure targets, and social engineering language) classify this message as a high-risk phishing attempt.

2. Evidence & Findings A. Headers (see attached email-header.txt) - SPF: softfail (sending IP 185.203.112.14 not authorized) - DKIM: none (no signature) - DMARC: fail (policy REJECT but message bypassed authentication) - Return-Path domain differs from legitimate Flipkart domains

B. Sender Analysis - From: order-update@flipkarrt-secure.com (typo-squatted) - Reply-To: support@flipkart.com (used to appear legitimate) - Spoofing indicators: domain typo-squatting, authentication failures, and VPS-hosted sending IP.

C. Links & Attachments - Displayed link text: "View Order & Verify Payment" - Actual href: http://flipkart-secure-checkout.in/login?uid=8934217 - Issues: insecure HTTP (no TLS), non-Flipkart domain, and personalized query parameter to feign legitimacy. - Attachment referenced: Invoice_8934217.pdf (do not open outside sandbox).

D. Email Content & Social Engineering - Urgency: "cancelled within 24 hours" — high-pressure tactic. - Threat: account suspension and cancellation used to coerce action. - Personalization: uses order number and recipient name to increase credibility.

E. Spelling/Grammar - No major typos in this sample, but suspicious structural and phrasing choices exist (e.g., generic signature, inconsistent branding).

3. Risk Rating Overall Risk: HIGH Rationale: Authentication failures (SPF/DKIM/DMARC), a mismatched/insecure link pointing to a non-official domain, and social-engineering pressure all indicate credential-harvesting intent.

4. Recommended Remediation - Do NOT click the link. Mark the email as phishing in your email client. - Block the domain flipkart-secure-checkout.in and monitor for traffic to the sending IP 185.203.112.14. - If credentials were entered, reset passwords and enable MFA on affected accounts. - Share the sample with your security operations team to update filters and protections.

5. Artifacts (included in the repository) - phishing_email.txt — raw email body (HTML) - email-header.txt — raw headers - sender-analysis.md — sender identity & spoofing analysis - header-analysis.md — SPF/DKIM/DMARC interpretation - Link-Analysis.md — link extraction and URL risk assessment

6. Notes / Limitations This analysis is based on a phishing-style sample. For full forensic attribution, perform WHOIS, TLS cert checks on landing domains, and sandbox URL detonation to observe payloads in a controlled environment.

Prepared by: Tarun Arulraj tarunarulraj23@gmail.com