Dharmin Tank Day 2 Task 2

Phishing Email Analysis Report

From: Apple Support <apple.security@support-apple.com>
Subject: Urgent! Your Apple ID has been locked.
Date: Thu, 30 May 2025 11:12:03 +0530

Dear Customer,

Your Apple ID has been temporarily locked for security reasons. We noticed unauthorized activity from a foreign IP address. Please verify your account within 24 hours or your Apple ID will be permanently locked.

Click here to restore your account: http://apple.support-verify-account.com/login

Thank you,
Apple Security Team

Phishing Indicators Found:

Phishing Characteristic	Observation
1. Spoofed Email Address	Email shows as `apple.security@support-apple.com`, not a legitimate Apple domain.
2. Mismatched URLs	Hyperlink displays as Apple, but leads to a suspicious domain: `support-verify-account.com`.
3. Urgent/Threatening Language	“Your Apple ID will be permanently locked” — invokes fear to prompt action.
4. Suspicious Link	URL is not HTTPS and not a genuine Apple domain.
5. Generic Greeting	“Dear Customer” — legitimate Apple emails usually address the user by name.
6. Grammar Issues	Minor errors in flow and punctuation.
7. Header Analysis Findings	`Return-Path`, `Reply-To`, and SPF/DKIM values do not match Apple’s infrastructure.
8. Unusual Sending Server/IP	Email originated from an unknown IP in Eastern Europe (based on header analysis).

Dharmin Tank Day 2 Task 2

Header Analyzed Using:

MXToolbox Email Header Analyzer : https://mxtoolbox.com/EmailHeaders.aspx

Conclusion:

This email displays multiple phishing characteristics such as spoofed addresses, suspicious domains, threatening language, and failed authentication checks in headers. It is likely a phishing attempt designed to steal Apple ID credentials.