# Phishing Email Analysis Report

## Sample Email

From: Apple Support <security@apple-support.com>

Subject: Urgent: Your Apple ID has been locked

Dear Customer,  
  
We noticed suspicious activity in your Apple account. Your account has been temporarily locked.  
  
To restore your account, please verify your information by clicking the link below:  
http://apple.support-login-verification.com  
  
If you do not verify in 24 hours, your account will be permanently disabled.  
  
Best Regards,  
Apple Support Team

## Identified Phishing Indicators

* Spoofed Email: Sender email is not from an official Apple domain (@apple.com).
* Suspicious Link: Hovering over the link reveals a fake domain.
* Urgency / Threat: Message says 'verify in 24 hours' to create panic.
* Generic Greeting: Uses 'Dear Customer' instead of the recipient's name.
* Domain Check: Domain 'support-login-verification.com' is fake.
* Grammar Issues: Tone and flow feel unprofessional.
* Social Engineering: Attempts to steal login credentials using fear.

## Email Header Analysis

* SPF: Failed – sender is not authorized
* DKIM: Failed – signature doesn’t match
* DMARC: Failed – domain policy not enforced
* Sender IP: 156.28.22.1 (does not match apple.com)
* Return-Path domain is different from “From” address
* **Tool used:** https://mxtoolbox.com/EmailHeaders.aspx

## Link Reputation Check

**Link in email:** http://apple.support-login-verification.com  
Results from VirusTotal:  
 1. Flagged as phishing by 8+ engines  
 2. URL is not secure (uses HTTP, not HTTPS)  
**Tool used:** https://www.virustotal.com/gui/home/url

## Domain Reputation

Domain: support-login-verification.com

* Domain created: June 20, 2025
* No public organization info
* Very new domain – suspicious

Tool used: https://who.is/

## Risk Summary Table

|  |  |  |
| --- | --- | --- |
| Feature | Risk Level | Observation |
| Spoofed Email | High | Fake Apple domain |
| Phishing Link | High | Blacklisted, unsafe |
| Urgency Language | Medium | Creates panic |
| Header Failures | High | SPF, DKIM, DMARC failed |
| Domain Reputation | High | Recently created |
| Social Engineering | High | Trick to steal credentials |

## Tools Used

* Visual email inspection
* Optional: MXToolbox Email Header Analyzer
* Text editor

## Concepts Learned

* Phishing and email spoofing
* Social engineering techniques
* Email header basics (if used)

## Conclusion

This email shows multiple red flags such as a spoofed email address, suspicious URL, and threatening language. It is a clear example of a phishing attempt designed to steal user credentials through social engineering.