Phishing Email Analysis Report

# 1. Basic Email Metadata

|  |  |
| --- | --- |
| From | support@apple.com |
| To | user@example.com |
| Subject | Urgent: Your Apple ID has been locked |
| Date | 24.06.2024 |
| Attachment | unlock\_form.html |
| Link in Body | http://appleid-verification-login.safe-connect.ru/ |

# 2. Header Analysis

Analysis performed using MxToolbox.

|  |  |
| --- | --- |
| From vs Return-Path | Return path not shown, may differ from visible sender |
| SPF/DKIM/DMARC | Likely fails or not present (requires raw header) |
| Sending IP | Unknown — IP lookup can reveal suspicious country or ISP |
| Spoofing Detected | Yes — domain uses apple.com, but not verified |

# 3. Suspicious Elements

|  |  |
| --- | --- |
| Sender Email | Pretends to be Apple support but likely spoofed |
| Link | URL looks like Apple but points to a suspicious .ru domain |
| Urgency | “Your Apple ID has been locked” — forces quick action |
| Threat | Mentions account will be “permanently disabled” |
| Attachment | unlock\_form.html may be a fake login form |
| Grammar | Language is formal, but could still be fake |
| Domain Mismatch | Real Apple links are under apple.com, not safe-connect.ru |

# 4. Summary of Phishing Traits Identified

- Spoofed sender using support@apple.com  
- Urgent language and threat of account lock  
- Mismatched URL and actual destination  
- Suspicious attachment mimicking a login form  
- Potentially malicious .ru domain  
- No signs of encryption or valid security headers

# 5. Final Conclusion

This email is a phishing attempt aimed at harvesting Apple ID credentials by tricking the user into clicking a malicious link and submitting login details in a fake form.  
  
Users should not click links or download attachments. The email should be reported and deleted immediately.

- VirusTotal or URLScan report on suspicious link (suggested action: upload link to virustotal.com or urlscan.io)