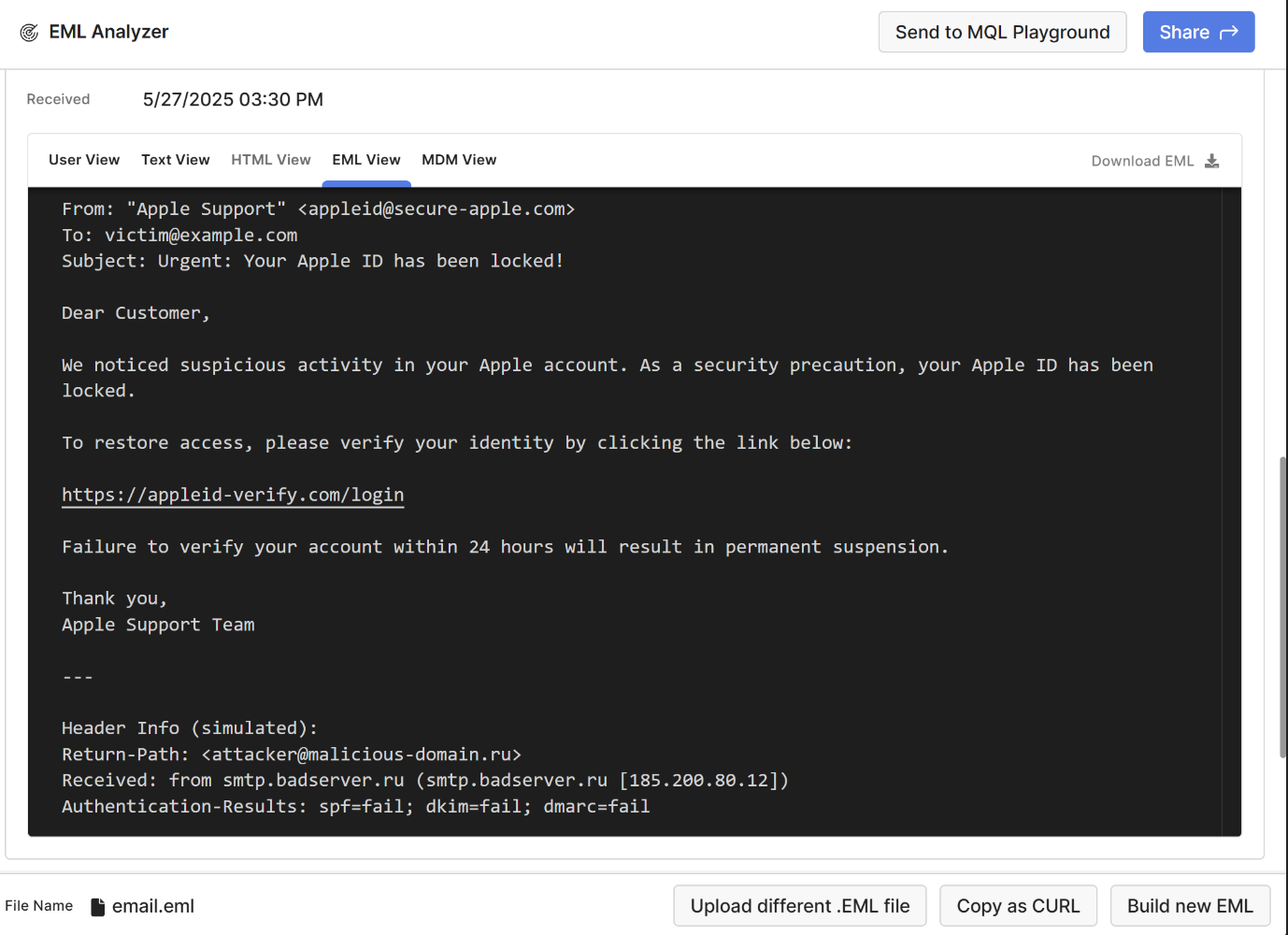
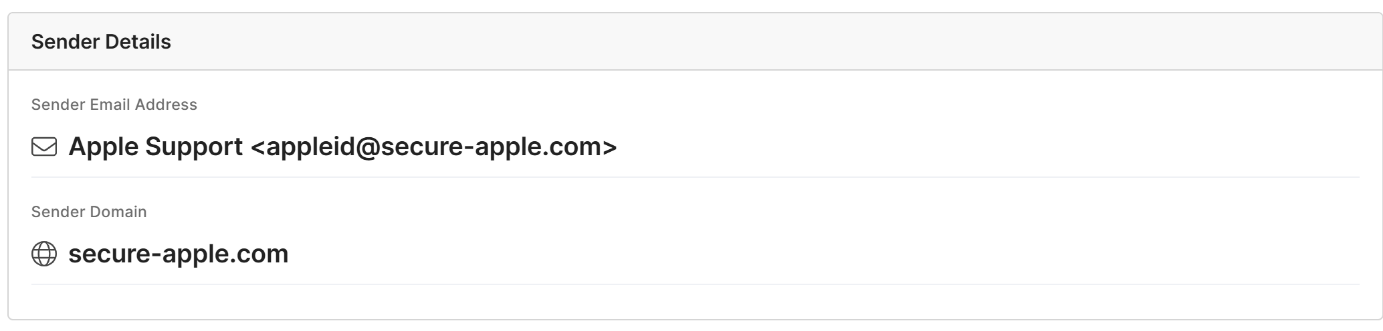
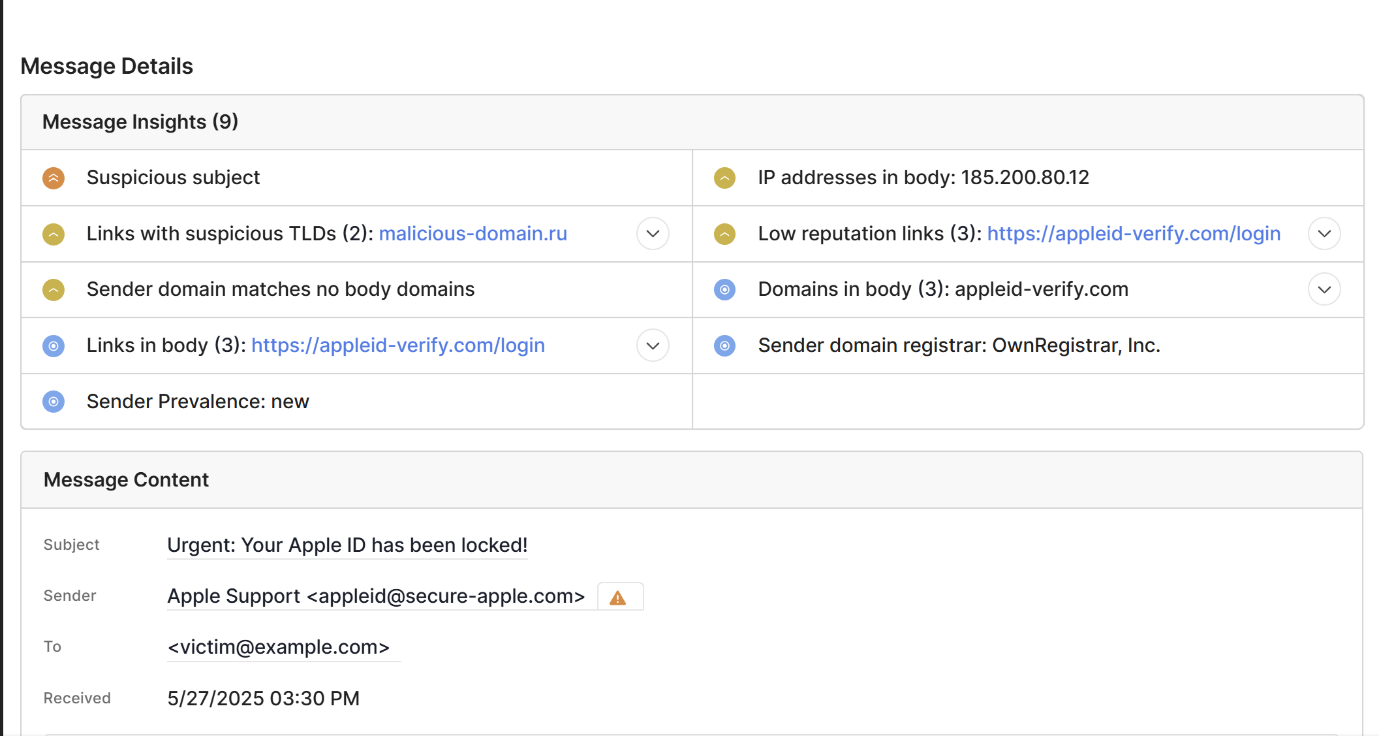
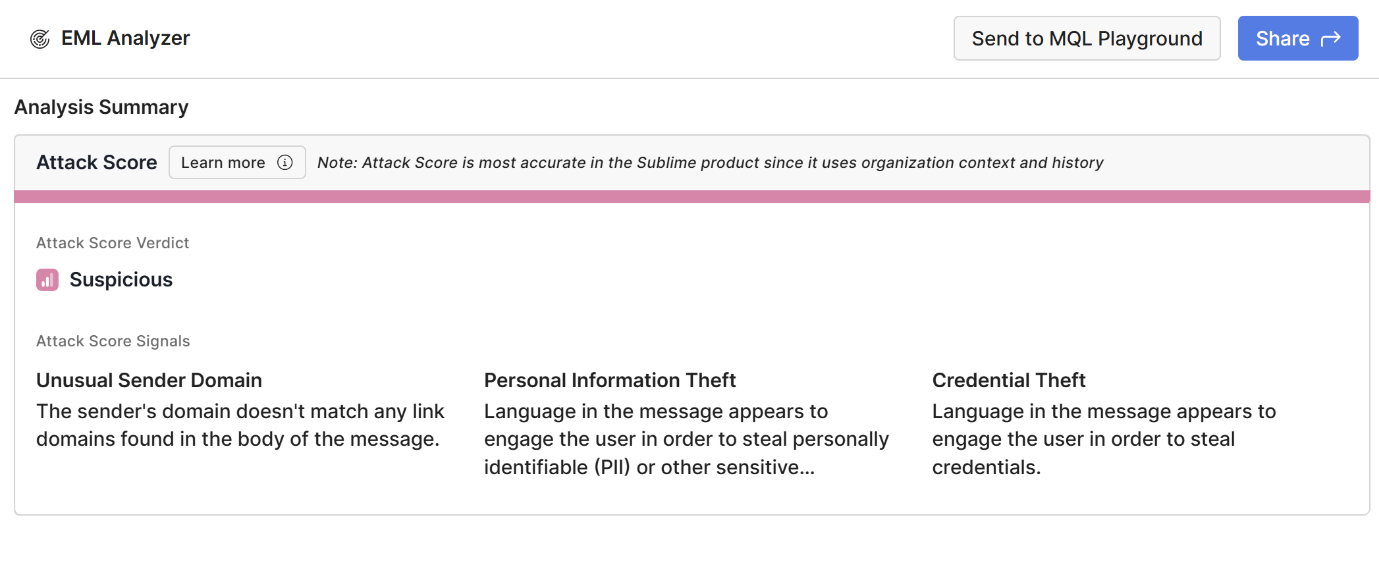
Analyzing phishing email

**These are the contents of a phishing email :**



**Using the tool EML ANALYZER, here are my findings:**



**Here’s a table about all the phishing indicators found:**

| **#** | **Phishing Indicator** | **Description** |
| --- | --- | --- |
| 1 | **Fake "From" Address** | Appears to be from Apple, but domain is secure-apple.com (not legitimate). |
| 2 | **Return-Path Mismatch** | Actual sender: attacker@malicious-domain.ru. Not Apple. |
| 3 | **Failed Authentication** | SPF, DKIM, DMARC all failed — domain not authorized to send this email. |
| 4 | **Suspicious URL** | Link goes to appleid-verify.com — not an official Apple domain. |
| 5 | **Urgent Language** | Creates panic: “locked,” “within 24 hours,” “permanent suspension.” |
| 6 | **Generic Greeting** | No personalization ("Dear Customer") — typical of phishing. |
| 7 | **Grammar and Formatting** | Plain design, lack of branding, potential errors. |
| 8 | **Unusual Sending Server** | Sent from suspicious IP (185.200.80.12) not used by Apple. |

**These were the findings from header of the email:**

Header Info (simulated):

Return-Path: <attacker@malicious-domain.ru>

Received: from smtp.badserver.ru (smtp.badserver.ru [185.200.80.12])

Authentication-Results: spf=fail; dkim=fail; dmarc=fail