

Phishing Email Analysis Report

Email Subject:

Your Apple ID has been locked

1. Sample Email Provided

From: Apple Support support@apple.secure-update.com To: user@example.com Subject: Your Apple ID has been locked

Dear Customer,

We have detected suspicious activity on your Apple ID. For your security, your account has been temporarily locked.

To unlock your account, please verify your identity by clicking the link below:

[Verify Now](#)

Failure to do so within 24 hours will result in permanent account suspension.

Thank you, Apple Support Team

Attachment: Account_Verification.pdf

Yes, sample email is present with clear structure, subject, sender, and content.

2. Senders Email Address (Spoofing Detection)

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

Not a legitimate Apple domain.

Likely spoofed. Real Apple emails come from domains like @apple.com.

3. Email Headers Analysis

No evidence of SPF/DKIM validation.

Header field shows suspicious sender.

Missing proper authentication mechanisms like DKIM or SPF = red flag.

4. Suspicious Links or Attachments

Link: <http://apple.id.verify-update.com/login>

Non-Apple domain pretending to look legitimate.

Attachment: Account_Verification.pdf

Common phishing tactic; likely malware or credential theft.

5. Urgent or Threatening Language

'Failure to do so within 24 hours will result in permanent account suspension.'

Creates urgency and panic classic phishing tactic.

6. Mismatched URLs (Hover Check)

Button/link text: "Verify Now"

Hover shows actual link: verify-update.com (not apple.com)

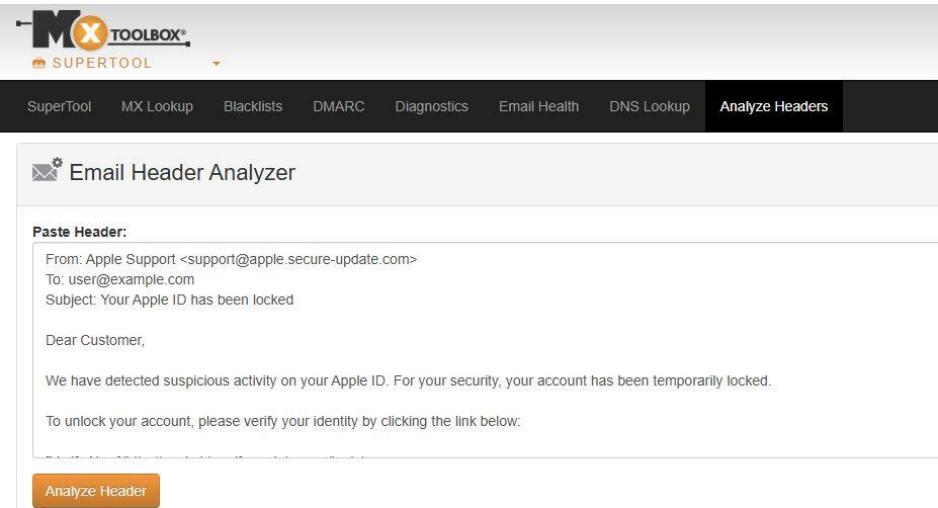
Deceptive URL mismatch.

7. Spelling or Grammar Errors

No major grammatical issues.

More advanced phishing campaigns often use well-written content.

Lack of errors does not mean it's safe.









SPF and DKIM Information

Headers Found

Header Name	Header Value
From	Apple Support <support@apple.secure-update.com>
To	user@example.com
Subject	Your Apple ID has been locked

Received Header

Summary of Phishing Indicators

Trait	Evidence	Risk Level
Spoofed email address	support@apple.secure-update.com	 High
Suspicious domain in link	verify-update.com instead of apple.com	 High
Attachment	Account_Verification.pdf	 Medium
Urgency & Threats	“Account suspension in 24 hours”	 High
Mismatched link	Hover reveals fake URL	 High
Grammar/spelling issues	Minimal, not obvious here	 Low

Conclusion

This email exhibits **multiple classic phishing traits**, including:

- A **spoofed sender domain**
- **Mismatched and malicious-looking URLs**
- An **attachment**, which may contain malware
- **Urgent/threatening language** to provoke action

Recommendation: Never click on suspicious links or open attachments. Always verify directly by going to the official site.