TASK-2

From: support@appleid.apple.com

Return-Path: security-alert@secure-appleid-login.com

Subject: IMMEDIATE ACTION REQUIRED - Apple ID Locked

Date: Wed, 06 Aug 2025 18:42:19 +0530

Dear Costumer,

We noticed suspicious activitie on your Apple ID and for security reasons we temporary locked you're account.

To unlcok and restore full access, please \*\*click the link below\*\* urgentely:

[www.appleid.com/verify](http://secure.appleunlock-help.com/login)

If you do not respond within 24 hours, your Apple ID will be \*\*permanantely suspended\*\* and all associated services and purchase will be inaccessible.

For your protection, we also recommend download the attachement below and run the included Apple Security Tool.

📎 Attachment: Apple\_Security\_Unlock.exe

Thank you for choosing Apple.

Apple Secure Support Team

**Display email-** Looks legit — but mismatches Return-Path domain

**Spelling errors-** "Costumer", "temporary", "urgentely", "permanantely" — unprofessional

**Suspicious link-** Hover text shows appleid.com, real link goes to secureappleunlock-help.com

**Urgent language-** “IMMEDIATE ACTION REQUIRED” and “permanently suspended” pressure users

**Malicious attachment**- .exe file claiming to be a security tool — high risk

**1. Sender & Return-Path Check**

* **From**: Appears legit (support@appleid.apple.com) but...
* **Return-Path**: security-alert@secure-appleid-login.com — not an official Apple domain.
* **Red Flag**: Mismatch between display and actual sender.

**2. SPF, DKIM, DMARC**

* **SPF**: Fail — sender IP not authorized by Apple.
* **DKIM**: None — no cryptographic signature.
* **DMARC**: Fail — domain alignment not met.
* **Red Flag**: All authentication checks failed.

**3. IP Trace**

* **IP**: 185.234.219.45
* **Use CLI tools:**

whois 185.234.219.45

host 185.234.219.45

* Result: IP belongs to a hosting provider in Eastern Europe, not Apple.
* **Red Flag**: Suspicious origin.

**Open-Source Tools You Can Use**

* **Email Header Analyzer (GitHub) -** Parse headers, trace hops
* **MXToolbox Analyzer -** Check SPF/DKIM/DMARC
* **ipinfo.io –** Trace IP origin
* **whois & host -** CLI tools for domain/IP lookup

**Summary**

- Sender: support@appleid.apple.com → Spoofed

- Return-Path: appleid@secure-appleid.com → Mismatch

- SPF/DKIM/DMARC: All failed

- IP: Eastern Europe hosting provider

- Link: http://secure-appleid.com/unlock → Fake Apple site

- Language: Urgent, fear-based

**1. What is Phishing?**

* A cyberattack where attackers impersonate trusted entities to steal sensitive data.
* Delivered via email, SMS (smishing), or voice (vishing).
* Example: Fake email from “Netflix” asking to update payment info.

**2. How to Identify a Phishing Email?**

* Spoofed sender address
* Generic greeting (“Dear Customer”)
* Urgent or threatening tone
* Suspicious links or attachments
* Spelling/grammar mistakes

**3. What is Email Spoofing?**

* Forging the sender’s address to appear legitimate.
* Exploits trust by mimicking known contacts or brands.
* Example: admin@micros0ft.com instead of admin@microsoft.com

**4. Why Are Phishing Emails Dangerous?**

* Can install malware or ransomware
* Steal credentials or financial data
* Lead to identity theft or business compromise

**5. How Can You Verify the Sender’s Authenticity?**

* Hover over sender address to check domain
* Use header analysis tools to inspect SPF/DKIM/DMARC results
* Contact sender via official website or phone

**6. What Tools Can Analyze Email Headers?**

| **Tool** | **Features** |
| --- | --- |
| [MXToolbox](https://mxtoolbox.com/EmailHeaders.aspx) | SPF/DKIM/DMARC checks, server hops |
| [Google Header Analyzer](https://toolbox.googleapps.com/apps/messageheader/) | Parses headers, shows delivery path |
| [Microsoft Header Analyzer](https://emailheaders.mhtools.net/) | Visualizes email flow |
| [Mailmodo Analyzer](https://www.mailmodo.com/tools/email-header-analyzer/) | Breaks down headers, flags suspicious signs |

**7. What Actions Should Be Taken on Suspected Phishing Emails?**

* **Do not click** links or open attachments
* **Report** to IT/security team or email provider
* Use “Report phishing” feature in Outlook/Gmail
* **Delete** the email after reporting

**8. How Do Attackers Use Social Engineering in Phishing?**

* Exploit human psychology: urgency, fear, trust
* Impersonate authority figures or known contacts
* Use personalized info from social media (spear phishing)