Phishing Email Analysis Report

# 1. Email Header Analysis

Return-Path: <domain@domain-name.com>  
Received: from mail.domain-name.com (mail.domain-name.com. [192.0.2.1])  
 by mx.google.com with ESMTP id abc123xyz  
 for <your@email.com>; Wed, 29 May 2025 10:00:00 -0700 (PDT)  
From: "National Security Department" <domain@domain-name.com>  
To: your@email.com  
Subject: Apple Facetime Information Disclosure  
Date: Wed, 29 May 2025 10:00:00 -0700  
Message-ID: <ABC123DEF456@mail.domain-name.com>  
MIME-Version: 1.0  
Content-Type: text/html; charset="UTF-8"

- Spoofed Sender Address: The sender uses a generic domain (domain-name.com), not a legitimate government domain (e.g., .gov).

- Fake Department: "National Security Department" is a fabricated entity to instill fear or urgency.

- Received Line: May be forged or relay from an untrusted domain.

# 2. Email Body Analysis

- Urgent Language: Mentions a vulnerability in Apple Facetime, creating panic and urgency.

- Social Engineering: Exploits fear by suggesting user's calls/videos may have been leaked.

- Suspicious Link: "Facetime Verification" link with no visible URL; likely a phishing site.

- Time Pressure: States that the verification site will be available for 72 hours to prompt quick action.

# 3. Phishing Indicators Summary

- Sender domain does not match a legitimate government agency

- Misleading department name to gain trust

- Use of urgency and fear to pressure user

- Embedded hyperlink disguised as a button

- Lack of personalized greeting or contact details

# 4. Conclusion

The email clearly exhibits multiple phishing indicators, including spoofed sender, misleading content, fear-based manipulation, and a malicious link. Users should avoid clicking the link and report the email to the appropriate authorities.

# 5. Recommended Actions

- Do not click on the verification link

- Report the email as phishing

- Block the sender's domain

- Educate users about similar tactics