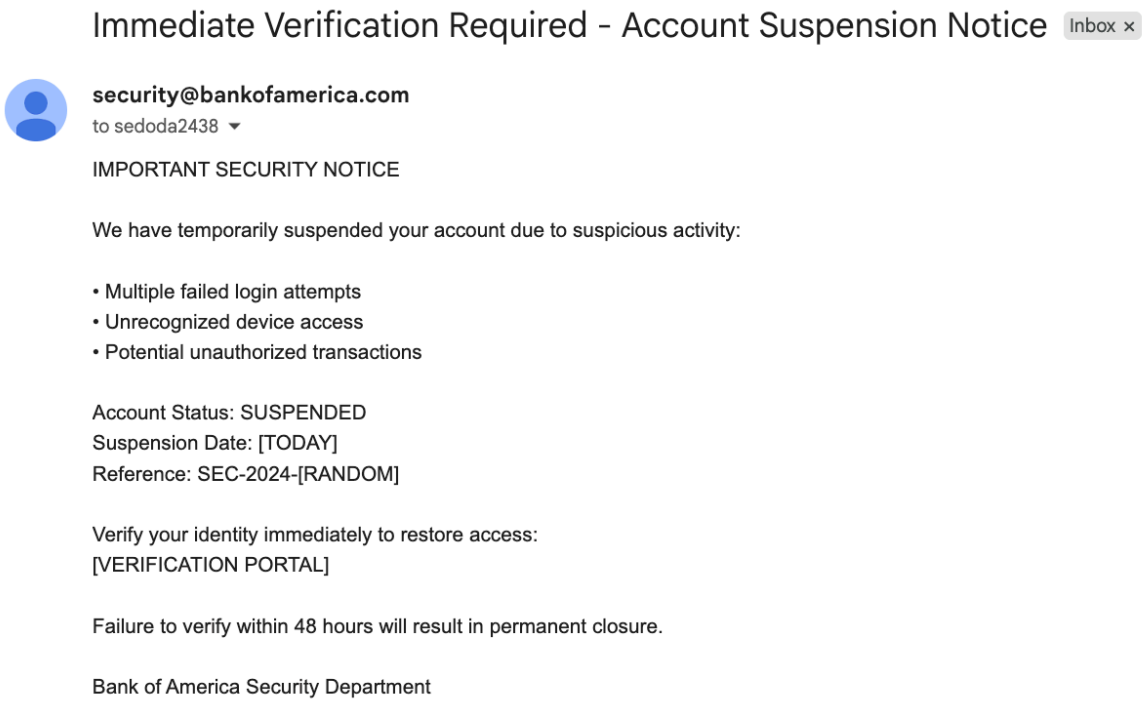
Report



1. General Overview

- **Subject:** *Immediate Verification Required – Account Suspension Notice*
- **Sender Display Name/Address:** `security@bankofamerica.com` (spoofed)
- **Recipient:** `sedoda2438@cerisun.com`
- **Date:** 23 September 2025

This email claims to be from Bank of America, warning of an account suspension due to "suspicious activity," urging the recipient to verify their identity.

Original message

Message ID	<175863924846.3869.11619087762241538615@bankofamerica.com>
Created on:	23 September 2025 at 20:24 (Delivered after 2 seconds)
From:	security@bankofamerica.com
To:	sedoda2438@cerisun.com, sedoda2438@cerisun.com
Subject:	Immediate Verification Required - Account Suspension Notice
SPF:	NONE with IP 0.0.0.0 Learn more

2. Indicators of Phishing

a) Technical Indicators

- **SPF Check:** `NONE with IP 0.0.0.0` → This shows the sender domain did not pass authentication. A legitimate Bank of America email would have valid SPF/DKIM/DMARC records.
- **Return Path & Received Headers:** Message originates from localhost (`127.0.0.1` / `10.244.2.108`) via Haraka, suggesting spoofing/testing rather than a genuine mail server.
- **Message ID:** Oddly formatted with `@bankofamerica.com` but generated outside legitimate infrastructure.

b) Content Indicators

- **Urgency:** "Failure to verify within 48 hours will result in permanent closure." → Classic scare tactic.
- **Generic Language:** No personalization (e.g., customer name/account number).
- **Suspicious Links:** Mentions "[VERIFICATION PORTAL]" but does not show a legitimate BoA link.

c) Stylistic/Formatting Issues

- Awkward phrasing ("SEC-2024-[RANDOM]").
- Overuse of capital letters ("IMPORTANT SECURITY NOTICE," "SUSPENDED").
- Fake reference numbers to look official.

3. Likely Goal of Attack

- Harvest **login credentials** by luring the user into clicking the "verification portal."
- Potentially collect **personal information** (PII) and/or financial details.
- Could also deliver **malware** if the link/file was malicious.

4. Risk Assessment

- **Severity: High** – Attempts credential theft.
- **Impact if successful:**
  - Compromise of banking credentials.
  - Potential financial fraud.

- Identity theft.

5. Recommendations

1. **Do NOT click** on any links or download attachments.
2. **Report the email** to your IT/security team and to the impersonated institution (Bank of America).
3. **Block the sender domain/IP** on your mail server.
4. **User Awareness:** Train recipients to recognize red flags (urgency, generic greeting, mismatched domains).
5. **Technical Controls:** Ensure SPF/DKIM/DMARC enforcement to reduce spoofed email delivery.

Conclusion:

This is a **phishing email** masquerading as a Bank of America security notice. It uses urgency, scare tactics, and spoofed sender information to trick the recipient into clicking a malicious verification link. It should be reported, quarantined, and blocked immediately.