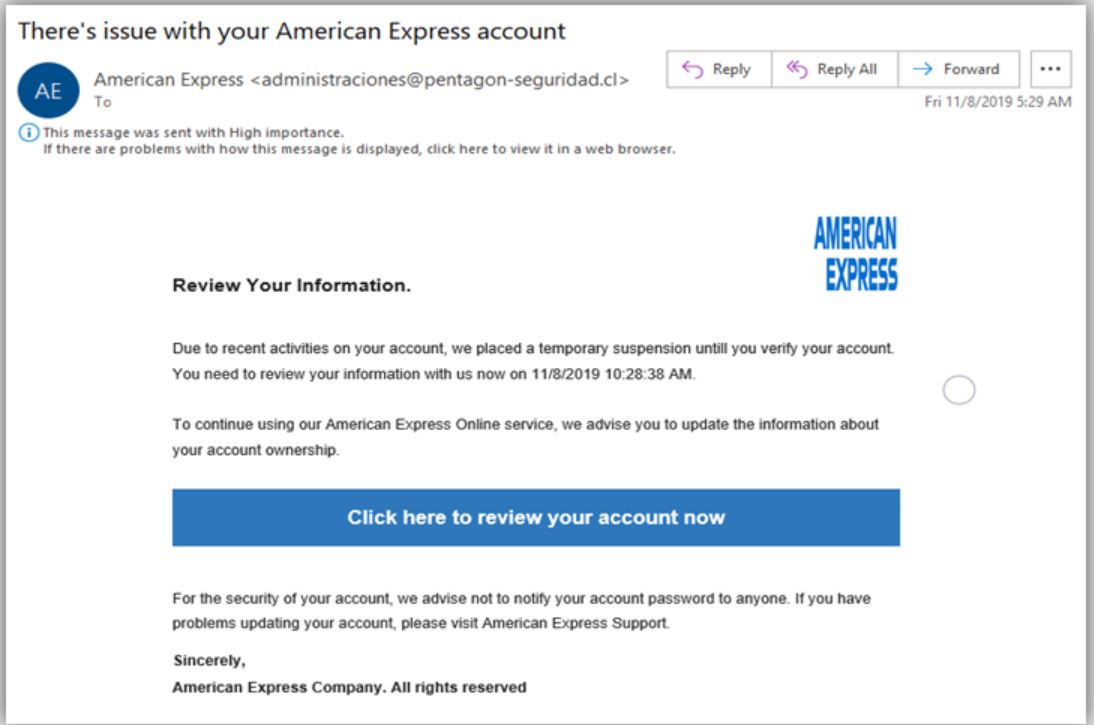
Phishing Email Analysis Report

# Sample Email Screenshot:



Subject: There’s issue with your American Express account

Sender: administraciones@pentagon-seguridad.cl

Company Impersonated: American Express

Time: Fri 11/8/2019 5:29 AM

# Step-by-Step Analysis

## 1. Sender’s Email Address Analysis

Email: administraciones@pentagon-seguridad.cl  
Suspicious domain (.cl, unrelated to Amex) and unrelated name (pentagon-seguridad).  
Conclusion: Spoofed or impersonating sender – RED FLAG.

## 2. Email Header Discrepancies

Due to screenshot format, raw headers can't be verified. But timing and domain mismatch suggests likely authentication failures.  
Conclusion: Potential SPF/DKIM/DMARC issues.

## 3. Suspicious Links or Attachments

CTA link: 'Click here to review your account now'. Hidden destination, but typical phishing behavior.  
Conclusion: Likely a malicious redirect to fake login.

## 4. Urgent or Threatening Language

Language: 'temporary suspension', specific timestamp.  
Conclusion: Social engineering tactic using urgency.

## 5. Mismatched or Fake URLs

Email domain does not match company. Link masked behind button.  
Conclusion: Likely mismatched or malicious URL.

## 6. Spelling & Grammar Errors

Examples: 'There’s issue', 'untill' with double L.  
Conclusion: Spelling and grammar errors indicate phishing.

## 7. Summary of Phishing Traits in This Email

| **Indicator** | **Description** |
| --- | --- |
| Sender Spoofing | Email from a domain unrelated to American Express |
| Urgency | Account suspension threat, time pressure |
| Grammar Errors | “There’s issue”, “untill” |
| Suspicious Link | Hidden under CTA button |
| Generic Greeting | No use of your name - not personalized |
| Visual Tricks | Uses logo and layout to fake legitimacy |