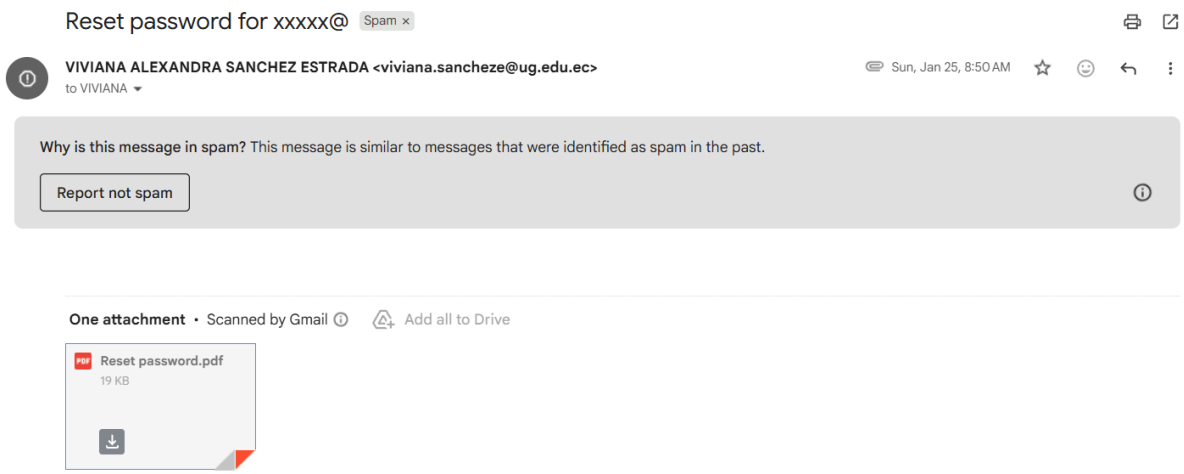
PHISHING EMAIL ANALYSIS REPORT :



1. Email Overview

- **Subject:** Reset password for xxxxx@
- **Sender Name:** VIVIANA ALEXANDRA SANCHEZ ESTRADA
- **Sender Email:** viviana.sancheze@ug.edu.ec
- **Folder Classification:** Marked as Spam by Gmail
- **Attachment:** Reset password.pdf (19 KB)

2. Sender Email Analysis

The email claims to be a password reset notification. However:

- The sender domain (**ug.edu.ec**) appears to be an educational institution.
- There is no clear relationship between the sender and the recipient's account.
- Legitimate password reset emails are usually sent from official service domains directly related to the platform.

3. Spam Classification

Gmail automatically flagged this email as spam and indicated it is similar to previously identified spam messages.

This suggests:

- The message structure matches known phishing/spam patterns.

- The sender reputation may be suspicious.

4. Subject Line Analysis

The subject line states:

“Reset password for xxxxx@”

Observations:

- The account reference appears incomplete.
- Password reset topics create urgency and concern.
- Attackers commonly use account security themes to trick users.

5. Attachment Analysis

The email includes a PDF attachment:

Reset password.pdf (19 KB)

Observations:

- Legitimate services typically provide secure reset links, not PDF attachments.
- PDF files can contain malicious links or redirect to fake login pages.
- The attachment was unsolicited.

6. Header Analysis

- The email was flagged as spam by Gmail’s filtering system.
- Spam classification often indicates authentication failure, domain reputation issues, or suspicious sending patterns.

7. Social Engineering Techniques Identified

The email likely uses:

- **Urgency:** Password reset implies immediate action.
- **Fear:** Suggests possible account compromise.
- **Authority Impersonation:** Uses an institutional-looking email domain.

These techniques are commonly used in credential-harvesting attacks.

8. Threat Classification

- **Type of Attack:** Credential Phishing / Possible Malware Delivery
- **Risk Level:** High

Reasons :

- Marked as spam
- Unsolicited password reset request
- Suspicious attachment
- Possible sender impersonation

PDF Details :

Reset password

Dear xxxx,

Your xxxxx@ account password expires today.

Use the following information to continue using the same password.

Keep the same password

Thank you
xxxxx@

This is a mandatory service email sent to xxxxx@