Phishing Email Analysis Report

# Email Sample

Google Workspace – Urgent Storage Alert (HTML Body Only)  
Source: https://github.com/LinkSec/phishing-templates/blob/main/emails/google-workspace/google-workspace-urgent-google-workspace-storage-alert-modified.html

# 1. Simulated Sender Info

From: Google Workspace <noreply@googl3-support.com>  
To: me@gmail.com  
Subject: Urgent: Your Storage Limit Has Been Reached

# 2. Email Layout & Design

- Official-looking design mimics Google Workspace  
- Uses logo, layout, colors similar to real emails  
- Includes a fake warning message: “Your account will be suspended if action is not taken.”

# 3. Content Analysis

- Psychological pressure: urgency, data loss threat  
- CTA button: “Verify Now”  
- Link placeholder: href="#" (attacker would insert malicious URL)

# 4. Technical Observations

- No email headers provided (From, To, Subject must be simulated)  
- No real domain links or attachments in this sample

# 5. Phishing Techniques Identified

- Spoofed branding  
- Threatening language  
- Urgent call to action  
- Placeholder for malicious link  
- Lack of sender verification

# Conclusion

This sample is a visual clone of a Google Workspace warning email, crafted to scare the recipient into clicking a malicious link. Although this file doesn’t contain a real link or header data, it clearly demonstrates the psychological and design techniques used in phishing attacks.