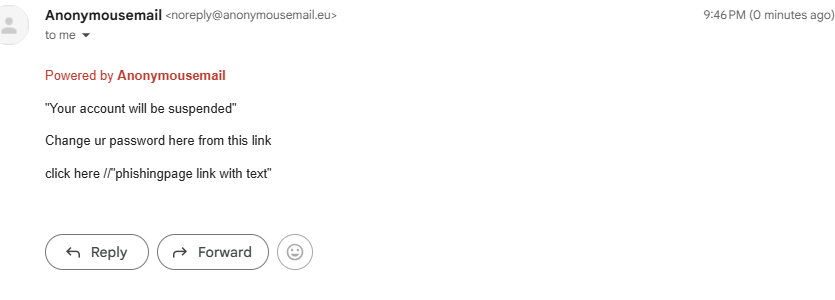
## PHISHING EMAIL ANALYSIS (Real-World Detail)

### **Sample Phishing Email**

**Example Email:**



**Purpose:**  
Tricks the user into clicking the link and entering their login info on a fake page.

**Examine Sender's Email Address**

**Check:**

Does the sender **name** look legit (e.g., "IT Support")?

Does the **domain** match the real company?  
 Real: [facebook@support.com](mailto:facebook@support.com)   
❌ Fake: [faccebook@suppoort.com](mailto:faccebook@suppoort.com)

Domain is unfamiliar or **slightly different**

Uses public email (e.g., @gmail.com) pretending to be official

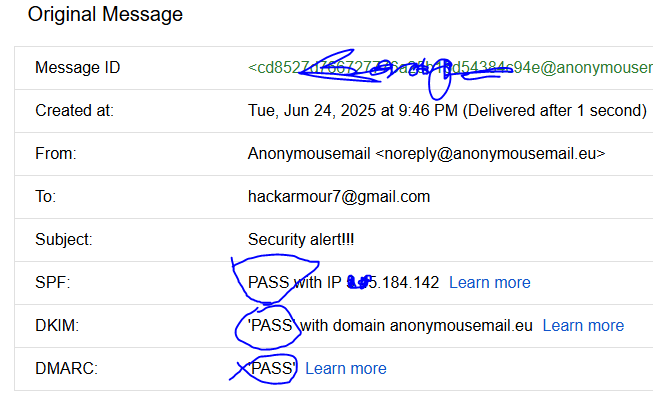
### **Check Email Headers**

**How To Check:**

In Gmail: Click **"Show Original"**

In Outlook: Right-click → **View Message Source**

Use mxtools to analyze



**Look For:**

Return-Path: Should match sender domain

Received: IP: Does it come from Microsoft or a random server?

SPF, DKIM, DMARC: If they say fail, it's suspicious.

**Example:**

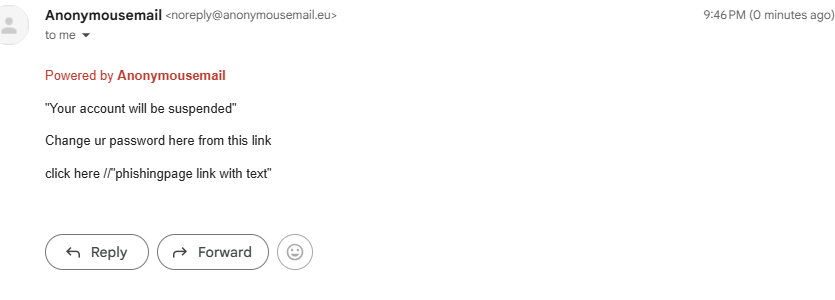
SPF: fail

DKIM: fail

DMARC: fail

### **Check Links and Attachments**

**Hover Over Links** (don’t click!)

* Text: Click here to verify
* Actual link: http://login-page.com → **Fake**
* ****

**Attachments:**

* File types: .doc, .xlsm, .zip, .exe
* Often contain **macros** or **malware** that infect your PC

**Use Tools:**

* [VirusTotal](https://www.virustotal.com/) to scan URLs or files

### **Check for Urgent or Threatening Language**

### **C:\Users\HP\AppData\Local\Microsoft\Windows\INetCache\Content.Word\anony mail.png**

**Common phrases:**

"Your account will be suspended"

"Immediate action required"

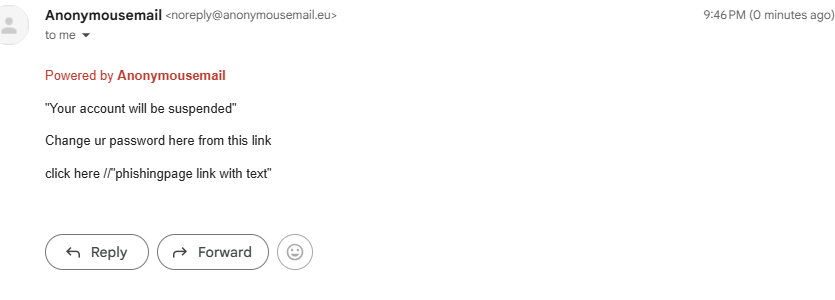
"Login from another country"

"Security alert"

**Why they use it:**  
To scare you into clicking quickly — **social engineering**.

### **Mismatched URLs (Link Trickery)**

**Looks like:**

* Text: “Click here ”
* Real: <http://loginpage.com>
* 

**Trick:**

Shows a safe name, but the real link is dangerous.

Attackers may even use text link

### **Spelling and Grammar Errors**

**Examples:**

“Verifiy your acount”

“Click hear”

“We suspens your account”

**Why it matters:**

Many phishing emails are written by non-native speakers or rushed.

**Note:** Some **targeted attacks** (spear phishing) may be well-written.

### **Summary: How to Spot Phishing**

| Red Flag | Example | Why It’s Suspicious |
| --- | --- | --- |
| **Fake sender domain** | @facebool-security-alert.com | Looks like facebook, but isn’t |
| **Bad links** | http://login-page.com | Takes you to a phishing site |
| **Urgency** | “Account has been suspended” | Makes you panic |
| **Hover link ≠ visible link** | Text says Microsoft, URL goes elsewhere | Link mismatch |
| **Spelling/Grammar issues** | “Suspencion” | Shows lack of quality |
| **Header failures** | SPF/DKIM = fail | Likely spoofed |