# 🛡️ Phishing Email Analysis – Fake PayPal Billing Notice

## Summary

This project documents a real-world phishing attempt targeting the user's PayPal account. The phishing email claimed a $351.24 Norton antivirus subscription had been purchased, urging the user to call a support number to dispute the charge.

---

## 🧠 Red Flags Identified

- \*\*Fake Sender Email:\*\* `njhfdsryiknbg45679@gmail.com`

- \*\*Non-personalized Greeting:\*\* “Dear EGAINES2007@GMAIL.COM”

- \*\*Suspicious Phone Number:\*\* Repeated multiple times, not traceable

- \*\*No matching invoice/bill number:\*\* Verified via Google

- \*\*Grammatical errors:\*\* Phrases like “going to deduct from your account”

- \*\*No previous Norton subscription purchased by user\*\*

---

## 🛠️ Detection Steps

1. Checked email headers and sender address

2. Cross-verified invoice and bill numbers online

3. Noticed poor grammar and urgency

4. Did not click any links or call any numbers

5. Deleted email and documented the attempt

---

## 🛡️ Recommended Controls

### Technical Controls

- Enable \*\*email filtering & spoof detection\*\*

- Configure \*\*DMARC/DKIM/SPF\*\* on email servers

- Use \*\*sandboxing\*\* for suspicious attachments

### Human Controls

- Train users on \*\*phishing red flags\*\*

- Promote a \*\*“think before you click”\*\* culture

- Encourage employees to \*\*report phishing\*\* using internal tools (e.g., Phish Alert Button)

---

## 📢 Incident Response in a Business Context

If this occurred within a company:

- Delete the email immediately

- Do not engage with the content

- Report to IT/Security team

- Notify affected stakeholders

---

## 🧾 Screenshot Evidence

