**E-Order#10 - Phishing Email Artifacts**

---

Sending Email Address: tdtfubihokcrxrcgbb@gmail.com

Subject Line: (no subject)

Recipient: wsquad101@gmail.com

Sending Server IP: 209[.]85[.]220[.]41

Resolve Host: mail-sor-f41.google[.]com

Reply To: tdtfubihokcrxrcgbb@gmail.com

Date and Time: Thu, 7 Aug 2025 11:20:21

Looking at this email that was sent to one of my personal addresses, this message is impersonating an invoice delivered by PayPal as well. The sender is informing the recipient about a fake recent purchase with a phone number included stating "Please call this number if the purchase was not authorized by you." The phishing email is also a form of social engineering in an attempt to have the user call the number listed and give out personal information such as credentials, financial information, or PII.

---

**Attached File Artifacts**

---

Attachment Name: Q940AYQ[.]pdf

SHA256: 58cbc883a47c1c0ab613aea4d3b33de87a4944274cb9413c116547a99e058a57

Phone Number Listed: +1 (810) 273-3491

Standard PDF file attached in a social engineering attempt. No embedded or malicious code to note.

---

**Suggested Defensive Measures**

---

As the sender is using a Gmail address, the most appropriate action would be to block this specific mailbox to prevent any more incoming malicious emails from this sender.