Eliza Styczyńska - Phishing Email Artifacts

Sending Email Address: uhhg93963@gmail.com

Subject Line: =?UTF-8?Q?Recibo_detallado_n=2E=C2=B0_Q940AYQ_con_?=
=?UTF-8?Q?fecha_2025/08/04_-_17=3A08_-_0YDY29AGWWX?= =?UTF-8?Q?=20?=

Recipient: wsquad101@gmail.com

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

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

Reply To: uhhg93963@gmail[.]com

Date and Time: Mon, 04 Aug 2025 17:24:55

Looking at the email personally sent to one of my addresses, this message is impersonating an invoice delivered by PayPal. The sender is informing the recipient about a fake recent purchase with a phone number included stating "If you did not authorize this transaction or you are unsure of the transaction, visit the Resolution Center below." The phishing email is 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:
58191B08D86895AABB82D236BF7030928E6DF9D6EEC06606014F83D89C9D7519

Phone Number Listed: +1 (855) 535-3217

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.