INITIAL REPORT (First 5 minutes)

Investigator: Mr_Chandan_Prasad

==

REPORT VERIFICATION:

Collected reported phishing email

Documented reporter's email (thehackersworld.indian@gmail.com)

Got timestamp of email (Nov 10, 2025 11:11 UTC)

Confirmed sender: support@paisabazaar.com

Noted location: Gmail spam folder

EMAIL PRESERVATION:

Saved original email

Exported full headers

Captured email content

Documented email folder location

Took screenshots of email

EMAIL HEADER ANALYSIS (5-10 minutes)

==================================

HEADER EXAMINATION:

Confirmed email headers available

Extracted Return-Path

Verified authentication (SPF: PASS, DKIM: PASS, DMARC: PASS)

Noted originating IP: 103.52.183.49

Identified mail server: mta5-183.49.ncdelivery04.com

SENDER VERIFICATION:

Verified sender domain: paisabazaar.com (REAL)

Confirmed sender: support@paisabazaar.com

Identified email service: NetcoreCloud Mailer

Checked for domain spoofing (None detected - REAL domain)

Verified domain legitimacy (Real financial services company)

AUTHENTICITY ASSESSMENT:

Email passes all authentication checks

Found urgency language ("Your Nov'25 Credit Score is Here!")

Identified personalization (Used name "Chandan")

Confirmed credential request via links

LINK & ATTACHMENT ANALYSIS (10-15 minutes)

===

LINK ANALYSIS:

Identified 3 malicious URLs

URL 1: https://delivery.paisabazaar.com/lt.pl?id=55590... (Main link)

URL 2: https://delivery.paisabazaar.com/lt.pl?id=55590... (Unsub)

URL 3: https://delivery.paisabazaar.com/lt.pl?id=55590... (Tracking)

Identified script: /lt.pl (Link tracking)

Purpose: Click tracking + Credential harvesting

ATTACHMENT ANALYSIS:

No attachments found

Content only: HTML email

Risk level: No malware payload

AFFECTED USER IDENTIFICATION

==

USER LISTING:

Identified recipient: thehackersworld.indian@gmail.com

Email personalized with: "Chandan"

Campaign type: Mass phishing (multiple recipients)

Status: Gmail spam folder (Blocked)

ACTION BY RECIPIENT:

Links NOT clicked (Safe)

Credentials NOT entered (Safe)

Email NOT opened from inbox (Safe - in spam)

CONTAINMENT ACTIONS
================================

EMAIL BLOCKING:

Email already in Gmail spam

No action needed (automatically blocked)

USER NOTIFICATION:

You are now aware (through this analysis)

Document provided

Training material created

DOCUMENTATION & ESCALATION
======================================

INCIDENT DOCUMENTATION:

Created incident report

Documented sender information

Listed all IOCs

Attached email headers

Included analysis findings

STATUS:

INCIDENT SAFE - No compromise

ANALYSIS COMPLETE - Training document created