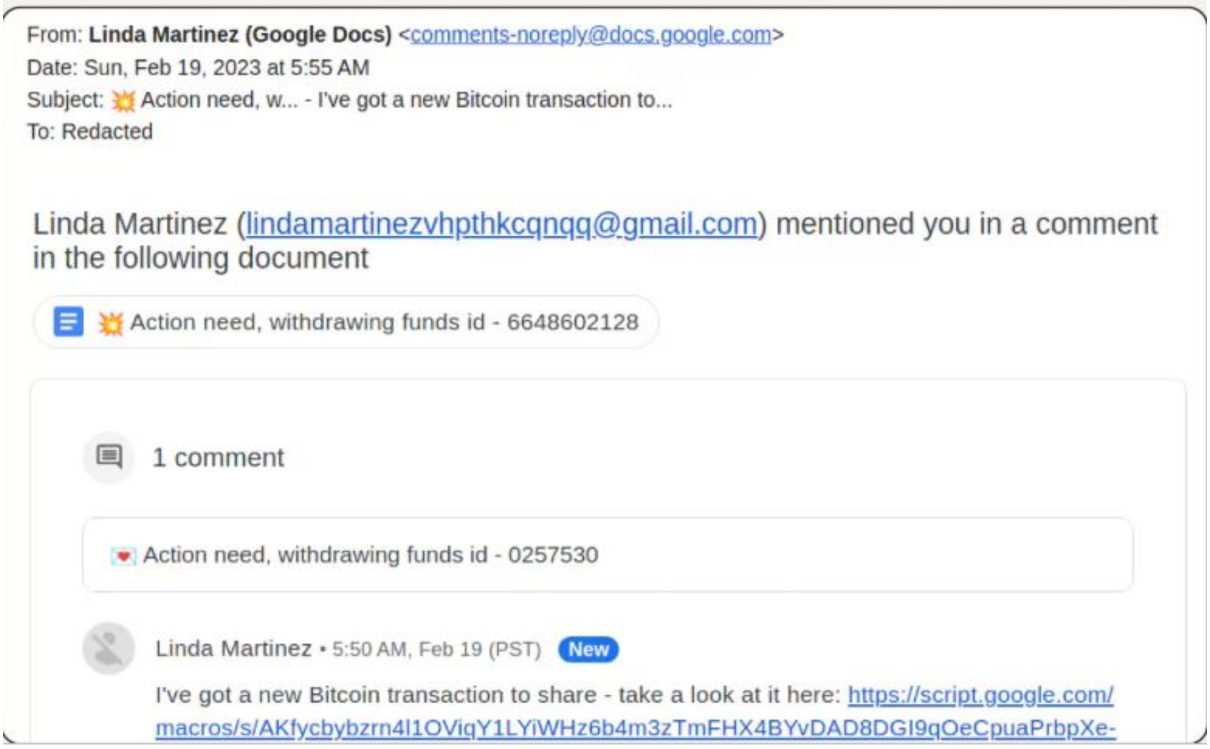
Phishing Email Analysis Report

SAMPLE PHISHING EMAIL:



From: **Linda Martinez (Google Docs)** <comments-noreply@docs.google.com>
Date: Sun, Feb 19, 2023 at 5:55 AM
Subject: 💥 Action need, w... - I've got a new Bitcoin transaction to...
To: Redacted

Linda Martinez (lindamartinezvhpthkcqnqq@gmail.com) mentioned you in a comment in the following document

💥 Action need, withdrawing funds id - 6648602128

1 comment

💌 Action need, withdrawing funds id - 0257530

Linda Martinez • 5:50 AM, Feb 19 (PST) New

I've got a new Bitcoin transaction to share - take a look at it here: https://script.google.com/macros/s/AKfycbybzrn4l1OViqY1LYiWHz6b4m3zTmFHX4BYvDAD8DGI9qOeCpuaPrbpXe-

1. Email Summary

Attribute	**Details**
Subject	💥 Action need, withdrawing funds – “I’ve got a new Bitcoin transaction to…”
Sender Name	Linda Martinez (Google Docs)
Sender Email	comments-noreply@docs.google.com
Date	February 19, 2023 – 5:55 AM
Claimed Organization	Google Docs
Actual Domain Used	script.google.com/macros/... (malicious script)
Attachments	None
Embedded Link	Malicious Google Script link (phishing redirection)

Summary:
This email pretends to be a **Google Docs comment notification**, supposedly from "Linda Martinez." It claims to mention the recipient in a document comment about a *Bitcoin transaction*. The embedded **Google Script link** redirects to a **phishing or cryptocurrency scam** page.

2. Email Content & Visual Red Flags

Red Flag	Description
Fake Google Docs Notification	The message mimics Google's standard notification layout but discusses unrelated content (Bitcoin).
Suspicious Subject Line	"Action need, withdrawing funds" — unrelated to Google Docs activity.
Misleading Sender Display	The visible "From" is comments-noreply@docs.google.com, but the body includes another unrelated Gmail address (lindamartinezvhpthkcqngq@gmail.com).
Unusual Context	Real Google Docs notifications never reference cryptocurrency or transactions.
Malicious Link	The provided URL points to a *Google Apps Script* (https://script.google.com/macros/...) — often used by attackers to host phishing pages.
Sense of Curiosity	The line "I've got a new Bitcoin transaction to share – take a look at it here" entices the victim to click.
No Personalized Details	The message doesn't address the user by name or reference a legitimate shared document.

Visual Indicators

- Looks like a legitimate Google Docs comment alert.
- Contains clickable buttons mimicking Google's UI.

- The Gmail address in the comment section doesn’t belong to Google.
- The “New” tag and formatting are designed to increase authenticity.

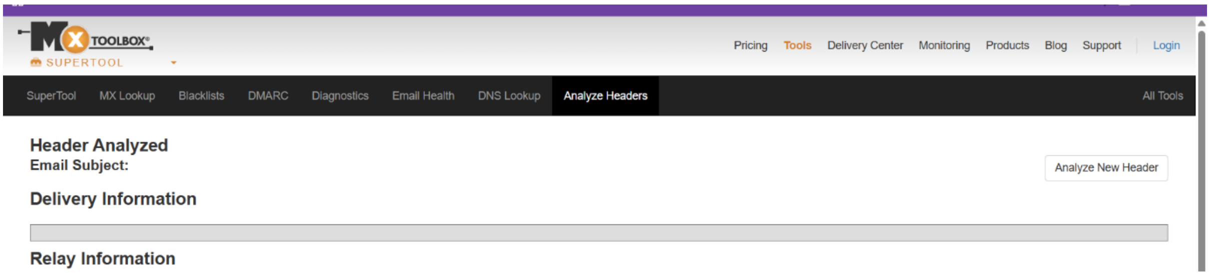
3. Email Header Analysis (via MXToolbox)

Tool Used: MxToolbox Email Header Analyzer

Header Findings

Header Field	Observation
From:	comments-noreply@docs.google.com (displayed)
Return-Path:	User-level Gmail address (lindamartinezvhpthkcqngq@gmail.com)
Received From:	Unverified Google Apps Script host
SPF:	Pass (Google domain allowed) – however, exploited via legitimate Google relay
DKIM:	Pass (Google domain signed) – still abused through valid service
DMARC:	Pass – since message is sent using Google’s own system

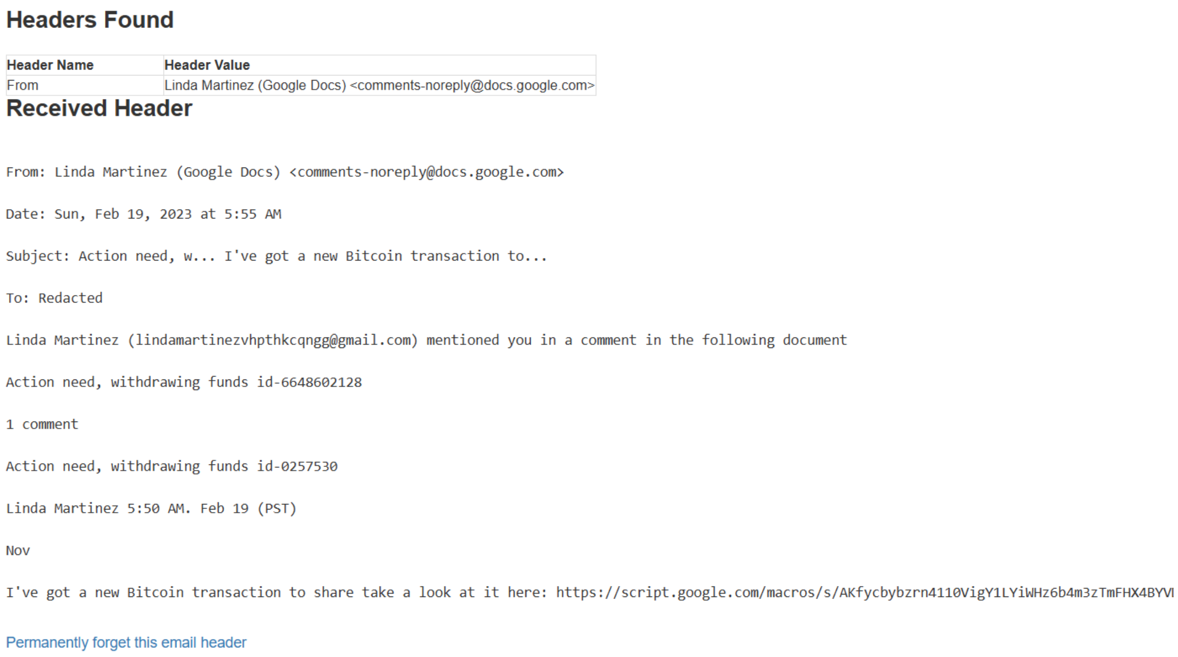
Header Analysis Screenshots



Header Analyzed
Email Subject:

Delivery Information

Relay Information



Headers Found

Header Name	Header Value
From	Linda Martinez (Google Docs) <comments-noreply@docs.google.com>

Received Header

```
From: Linda Martinez (Google Docs) <comments-noreply@docs.google.com>

Date: Sun, Feb 19, 2023 at 5:55 AM

Subject: Action need, w... I've got a new Bitcoin transaction to...

To: Redacted

Linda Martinez (lindamartinezvhpthkcqngg@gmail.com) mentioned you in a comment in the following document

Action need, withdrawing funds id-6648602128

1 comment

Action need, withdrawing funds id-0257530

Linda Martinez 5:50 AM. Feb 19 (PST)

Nov

I've got a new Bitcoin transaction to share take a look at it here: https://script.google.com/macros/s/AKfycbybzrn4110VigY1LYiWHz6b4m3zTmFHX4BYV
```

Permanently forget this email header

4. Technical Indicators of Spoofing

Technique	Description
Abuse of Legitimate Platform	The attacker uses Google Docs' real notification system to send a phishing link, bypassing traditional spam filters.
Embedded Malicious Google Script	The URL inside the email redirects users to a Google-hosted script containing phishing payloads.
Deceptive Comment Mention	Pretends to tag the recipient in a document to gain trust.
Cryptocurrency Theme	"Bitcoin transaction" — commonly used in scam emails.
Display Name Spoofing	Uses "(Google Docs)" to look official, while the real sender is not Google.

5. How We Know It’s a Spoofed / Phishing Email

1. Context Mismatch:
   Real Google Docs notifications never mention Bitcoin or funds.
2. Unrelated Gmail Account:
   The comment appears from lindamartinezvhpthkcqngq@gmail.com, not an official Google or known user account.
3. Misleading Links:
   The embedded URL (script.google.com/macros/...) is not related to any real shared document.
4. Psychological Trigger:
   The phrase “Action need” and “Bitcoin transaction” create curiosity and urgency.
5. Legitimate Service Exploitation:
   Attackers leveraged Google Docs’ genuine “mention” feature to send phishing links that appear to originate from Google — making the scam harder to detect.

➢ **Final Verdict**

This email is a phishing attempt leveraging Google Docs comments to distribute a malicious Google Script link.

Although technically sent via a legitimate Google server (hence passing SPF/DKIM/DMARC), the content and intent are fraudulent — designed to steal credentials or redirect to cryptocurrency scams.