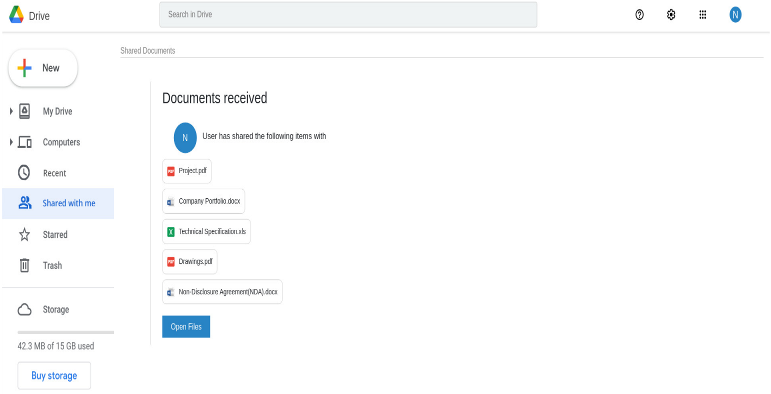
Phishing Analysis Report



Documents received

N User has shared the following items with

Project.pdf

Company Portfolio.docx

Technical Specification.xls

Drawings.pdf

Non-Disclosure Agreement(NDA).docx

Content:

The image shows a Google Drive screen with a user's storage usage, files shared with them, and a button to "Open Files."

Phishing Characteristics:

Mimicking Legitimate Interface: The image closely resembles a real Google Drive screen.

Urgency & Curiosity: The user is presented with valuable-looking files, creating a sense of urgency to open them.

Lack of Sender Verification: The source of the shared files is not explicitly stated.

Suspicious File Names: File names like "Non-Disclosure Agreement(NDA).docx" could be used to exploit trust and lure the user.

Possible Red Flags:

No Sender Information: The user is not provided with any information about who sent the files.

Lack of Metadata: Missing metadata can indicate manipulation or a fabricated image.

Suspicious File Types: The inclusion of multiple sensitive file types (PDF, DOCX, XLS) could raise concerns.

Recommendations:

Verify Sender: Always verify the source of shared files through email or other reliable channels.

Inspect File Metadata: Look for metadata information to confirm the file's origin and authenticity.

Exercise Caution: Be wary of unexpected files, especially if they contain sensitive information or come from unknown sources.

Conclusion:

This scenario exhibits several phishing characteristics, suggesting a potential phishing attempt. The lack of sender information, suspicious file types, and missing metadata should raise red flags. Users should exercise caution and follow the recommendations outlined above to avoid falling victim to a phishing attack.