Google Dorking Report

Query Used:
site:docs.google.com/spreadsheets/ "share"

Purpose: To identify publicly accessible Google Sheets containing the term “share” in order to highlight the types of data that can unintentionally be exposed to the public via search engines.

1. Methodology

- Performed a Google search restricted to the docs.google.com/spreadsheets/ domain.
- Reviewed search result snippets only, without downloading or modifying any content.
- Recorded only document titles and visible metadata from the Google results page.
- Sensitive details were redacted or generalized for privacy and compliance.

2. Findings Summary

No.	Document Title	Data Type Observed	Risk Level
1	Q4 Stock Market Analysis 2025	Stock market details, share performance scores	Medium
2	Employee Directory	Employee names, company emails, phone numbers	High
3	Company Financial Summary	Business metrics, possible revenue data	Medium
4	Automakers by Market Cap – 2025	Automotive sector market cap rankings	Low
5	Shareholder Report	Shareholder names, shares held	High

3. Observations

- Accidental Public Sharing: Many of the sheets appeared to be intended for internal use but were accessible to anyone with the link — and indexed by Google.
- Mixed Sensitivity: Some files were harmless public data (e.g., industry rankings), while others contained personally identifiable information (PII) such as employee contact details.
- Business Risk: Exposure of internal employee directories and shareholder data could lead to phishing, spam, or social engineering attacks.

4. Potential Impact

- Privacy Breach: Employee personal data could be exploited.
- Competitive Risk: Financial data and stock details could benefit competitors.

- Regulatory Compliance Issues: May violate GDPR, CCPA, or other privacy/data protection laws.

5. Recommendations

- Restrict Sharing Settings: Set Google Sheets to “Restricted” unless public access is intentional.
- Use Redaction: Remove or anonymize PII before making documents public.
- Periodic Audits: Regularly search your own domain using Google Dorks to find accidental exposures.
- Employee Training: Educate staff on risks of public sharing and how to properly configure permissions.
- Incident Reporting: If sensitive data is discovered, notify the affected company or data owner.

6. Conclusion

This search demonstrates how even a simple Google Dork can uncover sensitive corporate and personal information. Organizations must actively monitor and control their document-sharing practices to prevent unintentional data exposure.