



REPORT

USB Security Risk

Assessment

v1.2.0

Author:

Eldon Gabriel

July 9, 2025



Cybersecurity Professional | IT Security Consultant


TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
REVISION HISTORY.....	2
SECTION 1.0: USB SECURITY RISK ASSESSMENT.....	3
1.1 Project Description.....	3
1.2 Incident Overview.....	3
SECTION 2.0: APPROACH & ANALYSIS.....	4
2.1 Investigation Methodology.....	4
2.2 Sandboxed Investigation.....	4
SECTION 3.0: THREAT ANALYSIS.....	6
3.1 USB Contents.....	6
3.2 Potential Attack Scenarios.....	6
3.3 Risk Summary.....	6
SECTION 4.0: USB BAITING THREATS.....	7
SECTION 5.0: RISK MITIGATION RECOMMENDATIONS.....	8
5.1 Technical Controls.....	8
5.2 Policy and Awareness.....	8
SECTION 6.0: CONCLUSION.....	9
6.1 Key Takeaways.....	9
6.2 Security Implications and Recommendations.....	9



Cybersecurity Professional | IT Security Consultant

REVISION HISTORY

Version	Date	 Author	Description of Changes
v1.0.0	02/15/2025	Eldon G.	Initial draft.
v1.0.1	02/16/2025	Eldon G.	Fixed typos and improved sentence clarity
v1.1.0	02/16/2025	Eldon G.	Added cover page and expanded Risk Mitigation Recommendations.
v1.1.1	02/16/2025	Eldon G.	Enhanced Incident Overview section for clarity and technical depth.
v1.1.2	02/16/2025	Eldon G.	Enhanced Approach Analysis section for clarity and technical depth.
v1.2.0	07/09/2025	Eldon G.	Added full section structure, numbering, and conclusion.



Cybersecurity Professional | IT Security Consultant

SECTION 1.0: USB SECURITY RISK ASSESSMENT

1.1 Project Description

A USB drive was found at Rhetorical Hospital, raising concerns about a possible USB-baiting attack. A forensic team was called in to check for malware risks, review the files on the device, and test how well the hospital's USB security rules hold up.

1.2 Incident Overview

When I got to work, I found an unclaimed USB drive with the hospital's logo left behind. Knowing it could be a security risk, I picked it up and conducted a secure, controlled assessment. Inside, I found many files, both personal and work-related, including sensitive data and personal details.



Cybersecurity Professional | IT Security Consultant

SECTION 2.0: APPROACH & ANALYSIS

2.1 Investigation Methodology

The USB drive was examined in a sandboxed virtual environment to eliminate risk to the hospital's network. The investigation included:

- Physical inspection for tampering
- Mounting in read-only mode
- Scanning for malware, autorun scripts, and hidden files
- System monitoring for suspicious behavior

2.2 Sandboxed Investigation

A variety of files were recovered, including personal documents, images, and work-related materials. One folder included HR-related information, shift schedules, and employee contact details, heightening the data security concern. The presence of both personal and work files violated secure data handling practices.



Cybersecurity Professional | IT Security Consultant

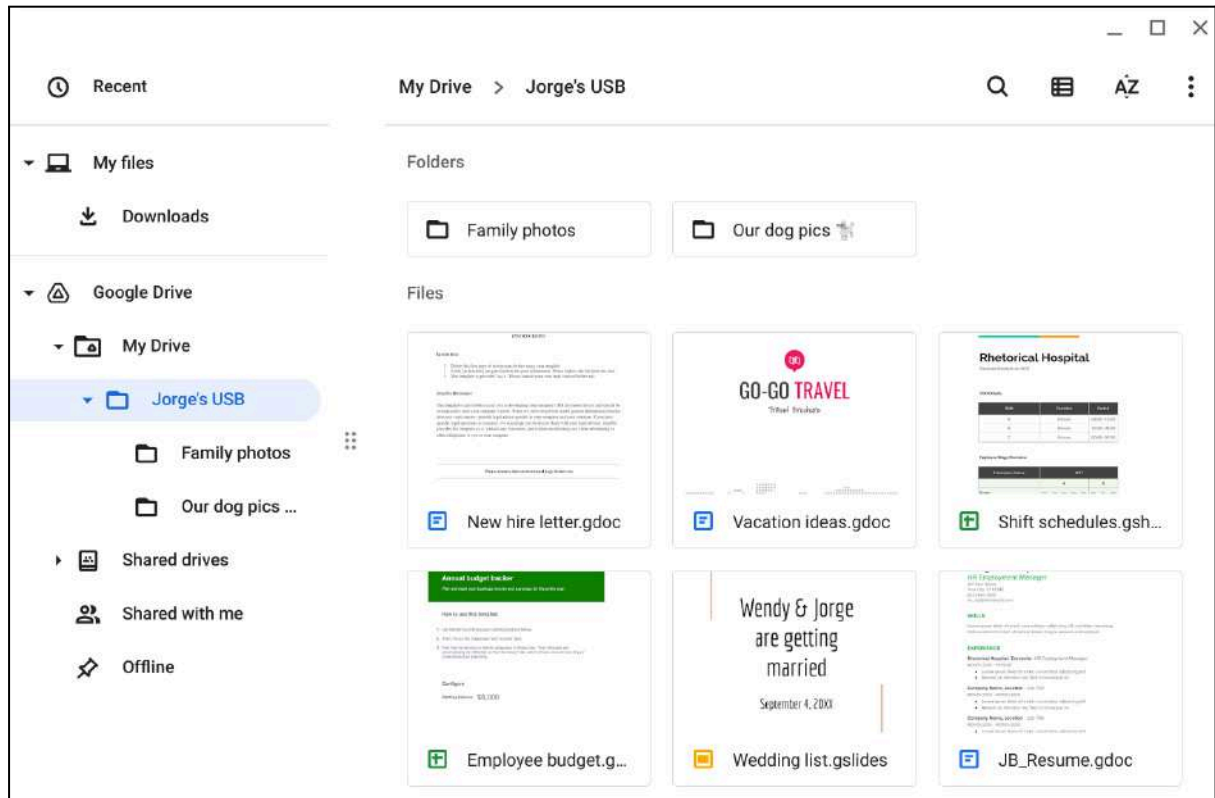


Figure 1: Screenshot of Jorge's USB file. Image source: Google, n. d., www.coursera.com



Cybersecurity Professional | IT Security Consultant

SECTION 3.0: THREAT ANALYSIS

3.1 USB Contents

Notable files included:

- HR documents (e.g., new hire letters, resumes)
- Shift schedules
- PII and internal hospital documents
- Family and personal photos

3.2 Potential Attack Scenarios

The USB could have been used for:

- Deploying malware (keyloggers, RATs, ransomware)
- Gathering credentials for internal access
- Launching phishing campaigns using data on the drive

The files may have been intentionally planted as decoys. If connected to a trusted workstation, this could have triggered malware installation or a persistent backdoor.

3.3 Risk Summary

Threat	Impact
Malicious USB Infection	<i>Malware execution across the hospital network</i>
Data Exposure	<i>Unauthorized access to hospital PII</i>
Social Engineering Attack	Phishing based on leaked personal data



Cybersecurity Professional | IT Security Consultant

SECTION 4.0: USB BAITING THREATS

USB baiting remains a common tactic used by attackers. This scenario illustrates its risk when a device is discovered and unknowingly plugged into a corporate environment. Key concerns include:

- **Hidden malware** inside benign-looking files
- **Ransomware payloads** disguised as documents
- **Social engineering hooks** via embedded personal data



Cybersecurity Professional | IT Security Consultant

SECTION 5.0: RISK MITIGATION RECOMMENDATIONS

5.1 Technical Controls

- **Encrypt sensitive data** at rest and in transit
- **Enforce access controls** using RBAC
- **Deploy endpoint protection** to scan USB devices
- **Replace outdated protocols** (e.g., disable autorun)

5.2 Policy and Awareness

- **Restrict USB usage** unless explicitly authorized
- **Implement a clear USB device policy** across departments
- **Train employees** on phishing, baiting, and suspicious device handling
- **Develop an incident response plan** for physical device threats



Cybersecurity Professional | IT Security Consultant

SECTION 6.0: CONCLUSION

6.1 Key Takeaways

- The USB contained both sensitive and personal data, violating secure data storage practices.
- Attackers may leverage such drives to infiltrate networks or harvest data.
- An isolated, secure analysis prevented possible compromise.

6.2 Security Implications and Recommendations

- Enforce strict USB access policies and encryption standards.
- Increase awareness and training on USB-related threats.
- Establish a formal process for reporting and investigating found devices.

Rhetorical Hospital must take proactive steps to mitigate risks associated with physical USB threats. This incident highlights the importance of secure device handling and continuous staff education in maintaining a robust cybersecurity posture.