Risk Management Analysis Report

Name: Esomchi Eze

1. Attack Matrix

The table below outlines possible threats, their causes, and impacts on my personal computer.

Threat	Hackers	Malware	Physical Thieves	Phishing Actors	Human Error
Physical loss			Physical Theft		Accidental damage
Denial of service (DOS)	DDoS Attack	Malware attack			
Disclosure	Data breach due to weak passwords	spyware		Identity theft	Unsecured file sharing
Forgery	Fake software	Malicious script		Fake invoices	Accidental edits

2. Risk Matrix

This table identifies key assets, and the risks associated with them.

Asset	Physical Damage	DOS	Human Error	Disclosure	Subversion
Personal Files	✓ Hard drive failure	✓(corruption)	✓ (Accidental deletion)	✓ (Data breach)	✓(Ransomware)
School Documents	✓Corrupted storage		✓ (Forgotten backups)	✓ (unauthorized access)	✓(Malware)
Stored Passwords	✓Laptop theft		✓ (Weak passwords)	✓ (keyloggers)	
Email Accounts		✓ (Server crash)	✓ (Sharing credentials)	✓ (credential leak)	✓(Hijacking)

3. Risk Identification

Based on the matrices, the three biggest risks are:

- Data Theft: Identity thieves can steal sensitive data if not properly secured.

- Unauthorized Access: Weak passwords or phishing attacks could allow hackers to access my personal accounts.

- File Loss: Without proper backups, important files could be permanently lost due to theft or damage.

Additionally, some other risks include:

- Malware Infection: Downloading unsafe files can lead to system corruption and data loss.

-Email Compromise: Phishing attacks can lead to unauthorized access to email and associated services.

4. Risk Probability Calculation

This table assesses the likelihood and impact of identified risks.

Asset	Attack	Impact	Likelihood	Significance
Personal Files	Ransomware Attack	€1,500	0.0490	€73.50
School Documents	Unauthorized Access	€2,000	0.0833	€166.60
Stored Passwords	Account Takeover	€800	0.3333	€266.64
Email Accounts	Phishing Attack	€300	0.0208	€6.24

5. Follow-up Measures

To minimize risks, I will take the following steps:

- Use strong, unique passwords and enable two-factor authentication.

- Regularly update software to patch security vulnerabilities.

- Backup important files using cloud/GitHub or external storage devices.

- Be cautious with emails and links to avoid phishing scams.

- Encrypt sensitive data where necessary to prevent unauthorized access.

6. Summary

This report made me more aware of the various risks that my personal computer faces. I realized the importance of strong cybersecurity measures, such as unique passwords across all sites, password management, backups, and vigilance against phishing attacks. Moving forward, I plan to enhance my security practices to better protect my data and digital assets.