COMPREHENSIVE AUDIT OF MY CYBERSECURITY PRACTICES

My primary focus in cybersecurity is on password protection and multi-factor authentication. I ensure that my passwords are updated regularly and rely on a password manager for added security.

I keep my devices updated with the latest Windows updates and Kaspersky antivirus. Additionally, I make sure all my smart devices are patched and updated as needed.

I frequently encounter phishing attempts, mostly via email, which I either delete or completely ignore. I also avoid opening emails from unknown senders.

For data security, I back up important files to at least two external drives. However, I haven't yet implemented data encryption, which is an area I'd like to improve.

In terms of encryption I Intend to imbibe the following

**Full Disk Encryption (Protects Your Entire Hard Drive)**

* **Windows:** [BitLocker](https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview) (built-in)
* **Mac:** [FileVault](https://support.apple.com/en-us/HT204837) (built-in)
* **Linux:** LUKS (via **Cryptsetup**)

**2. External Drive & Backup Encryption**

* **VeraCrypt** (Free, open-source, supports Windows/Mac/Linux) – Strong encryption for USB drives and external hard drives.
* **BitLocker To Go** (Windows) – Encrypts USB drives easily.
* **AxCrypt** (Windows/Mac) – Simple file and folder encryption.

https://github.com/Idahosadave/3mttProject/blob/045db865aba4cad29e5b0e5e8baa6793280d63c0/COMPREHENSIVE%20AUDIT%20OF%20MY%20CYBERSECURITY%20PRACTICES.docx