Security Checklist

1. Encrypted USB Stick for Passwords

   - Encrypt USB stick with strong encryption (e.g., AES-256)

   - Store passwords securely in an encrypted password manager on the USB stick

   - Keep USB stick in a secure, physically protected location

2. SIM-Less Phone for 2FA Apps

   - Use a phone without a SIM card for 2FA apps

   - Install 2FA apps (e.g., Google Authenticator, Authy, etc.) on this device

   - Secure the phone with a strong password and biometric authentication (if possible)

3. Secret Email for 2FA Backup

   - Create a separate email for 2FA backup (not linked to other accounts)

   - Enable strong 2FA (preferably with hardware key) on this email account

   - Store login details and recovery options in a secure location (e.g., encrypted USB stick)

4. Dedicated Offline Drive for Backups

   - Use a dedicated offline external drive for backups (no internet connection when not in use)

   - Encrypt the backup drive with strong encryption

   - Keep the offline drive in a secure location

5. Paper Backups of Passwords

   - Write passwords on paper, not digitally stored

   - Store paper backups in secure locations (e.g., safe or locked drawer)

   - Do not leave backups accessible or in public areas

6. Separate Email for Banking (Fully Isolated)

- Create a unique email address for banking purposes
- Do not link this email to other accounts or social media
- Use 2FA with hardware authentication (e.g., Yubikey) on this email account

7. Yubikey for Primary Authentication

- Use Yubikey (or similar hardware security key) for primary 2FA on supported accounts
- Store Yubikey in a secure location (e.g., safe or lockbox)
- Use Yubikey with all accounts that support hardware authentication

8. High-Security Accounts Linked to Hardware Authentication

- Ensure high-security accounts (e.g., banking, email, sensitive services) are only linked to hardware authentication
- Set up a backup process for account recovery via the secret email, if required
- Regularly check that hardware authentication is working and up-to-date

9. Linux or MacOS on Desktop/Laptop Secured with Password

- Set a strong password for Linux or macOS desktop/laptop accounts
- Enable full disk encryption (e.g., LUKS for Linux, FileVault for macOS)
- Keep the operating system and software updated to the latest security patches