**Name:** Bashar Tukur Shehu **Fellow ID**:FE/23/70792034 **Cohort:** Cohort 3

**Personal Cyber Hygiene Audit Report**

**1. Assessment of Current Practices**

**Passwords and Authentication:**

* Most passwords are unique but not regularly updated.
* MFA is enabled on all services.

**Device Security:**

* Antivirus and firewall are active on some devices.
* OS and applications are updated regularly, but some apps auto-update is disabled.

**Social Media Privacy:**

* Privacy settings are configured, but profile information is still somewhat visible.
* Occasional oversharing, but regular review of settings is not maintained.

**Email Practices:**

* Can recognize phishing attempts, and I verify links before clicking.
* Suspicious emails are deleted, but reporting to service providers is not done consistently.

**Data Backup:**

* Important files are backed up from time-to-time but not encrypted.
* Cloud storage is used, but no offline backup exists.

**2. Risk Analysis**

* **High Risk:** Weak password management and lack of regular updates.
* **Medium Risk:** Social media oversharing and infrequent backup encryption.
* **Low Risk:** Device security is mostly strong, but email verification needs improvement.

**3. Action Plan**

* **Passwords:** Use a password manager and update passwords every 3 months. Enable MFA on all accounts.
* **Device Security:** Enable automatic updates for all software and applications.
* **Social Media:** Conduct a privacy review monthly and limit shared information.
* **Email Practices:** Always verify links before clicking and report phishing emails.
* **Data Backup:** Encrypt backups and maintain an offline backup.

**4. Monitor and Review**

* **Bi-Weekly Check:** Review password manager and update weak passwords.
* **Monthly Review:** Reassess social media privacy settings and data backup status.
* **Quarterly Security Audit:** Check MFA settings and verify system updates.