**Personal Cybersecurity Audit and Remediation Plan**

**Learner Name: Muhammad Saad Shaikh**

**Date:05/06/2024**

**1. Inventory of Digital Assets**

List all your digital devices and online accounts below:

**Digital Devices:laptop, phone**

* Device 1: smart phone (Redmi Note 12)
* Device 2: Macbook (MacBook Pro (13-inch, Mid 2012)

**Online Accounts:**

* Account 1: Social Media (instagram, snaochat and TikTok)
* Account 2: Email, (Gmail)

**2. Password Audit**

Check the strength of your passwords and document any accounts with reused or weak passwords.

**Accounts with Weak/Reused Passwords:**

* Account 1:instagram
* Account 2: Tiktok
* ...

**Actions Taken: I added in MFA as well using an authenticator app for verification**

* Changed Passwords: Yes/No
* Implemented Password Manager: Yes/No (If yes, which one?)

**3. Update and Patch**

List any devices or applications that are outdated and need updates.

**Devices/Applications Needing Updates:**

* Device/Application 1:NA
* Device/Application 2: NA
* ...

**Actions Taken:**

* Updated Devices/Applications: Yes/No
* Notes: All my devices are up to date

**4. Two-Factor Authentication (2FA)**

Identify which accounts support 2FA and document if it's enabled.

**Accounts Supporting 2FA: Instagram,Tiktok,snapchat and Gmail**

* Account 1: 2FA Enabled: Yes/No
* Account 2: 2FA Enabled: Yes/No
* ...

**Actions Taken:**

* Enabled 2FA on Accounts: Yes/No
* Notes: I have 3 different ways to verify my identity with SMS text verification, using an authenticator app and back up codes

**5. Educate Yourself on Phishing**

Summarize key indicators of phishing attempts you learned.

**Key Indicators of Phishing:** 1. Inconsistencies in Email Addresses, Links & Domain Names

1. Really bad spelling, punctuation and grammar
2. Suspicious links and attachments
3. Threats or a sense of urgency

...

**Actions Taken: added in a filter to filter out spam and suspicious emails**

* Reviewed and applied knowledge to identify phishing: Yes/No
* Notes: Never click on any random links sent, always double check email domains, ignore, block and delete any suspicious emails

**6. Device Security Check**

Ensure devices have locks and security software installed.

**Device Security Status:**

* Device 1: Lock Enabled: Yes/No, Security Software: Yes/No
* Device 2: Lock Enabled: Yes/No, Security Software: Yes/No
* ...

**Actions Taken:**

* Enabled Locks/Installed Security Software: Yes/No
* Notes: on my phone and my laptop I use a strong password with more than 8 characters, a combination of numbers and special characters to protect my data and devices

**7. Privacy Settings Review**

Review and adjust the privacy settings on your online accounts.

**Privacy Settings Adjusted:**

* Account 1: Adjustments Made: Yes/No
* Account 2: Adjustments Made: Yes/No
* ...

**Actions Taken:**

* Adjusted Privacy Settings: Yes/No
* Notes: Never save any personal details such as financial information

**Conclusion and Next Steps**

Summarize the overall improvements you've made to your cybersecurity posture and any additional steps you plan to take in the future.

**Summary of Improvements: Added in extra security measures such as strengthening passwords and adding MFA**

**Planned Future Actions: I Will change devices and get a new phone and laptop in the future**