**Personal Cybersecurity Audit and Remediation Plan**

**Learner Name: Akshaj Pathak**

**Date:04-03-2025**

**1. Inventory of Digital Assets**

List all your digital devices and online accounts below:

**Digital Devices:**

* Device 1: HP Laptop | intel i5 processor, 512Gb SSD, 16Gb RAM | windows 11 operating system
* Device 2: Samsung Galaxy M33 smartphone | Android version 14

**Online Accounts:**

* Account 1: Email: akshajp545@gmail.com, Google
* Account 2: Email: akshajp54@gmail.com, Google

**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: akshajp545@gmail.com
* Account 2: akshajp54@gmail.com

**Actions Taken:**

* Changed Passwords: Yes
* Implemented Password Manager: Yes. The password manager used was Kaspersky. Passwords for both the accounts had moderate strength and could be cracked with some effort. Therefore it was suggested to change the passwords and make stronger passwords for both the accounts

**3. Update and Patch**

List any devices or applications that are outdated and need updates.

**Devices/Applications Needing Updates:**

* Device/Application 1: NO
* Device/Application 2: NO

**Actions Taken:**

* Updated Devices/Applications: Yes
* Notes:
* Device 1- laptop’s latest updates have been successfully installed 20 days ago and the device notifies me about any of the latest updates to the software or operating system
* Device 2- smartphone’s latest updates have been successfully installed 1 month ago and the device notifies me about any of the latest updates to the software

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

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

**Accounts Supporting 2FA:**

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

**Actions Taken:**

* Enabled 2FA on Accounts: Yes
* Notes: Two-Factor Authentication is enabled for account 1 (the main account) however it is disabled for account 2 (the recovery account). It is enabled on account 1 through a passkey / security key, google prompt and through my verified phone number

**5. Educate Yourself on Phishing**

Summarize key indicators of phishing attempts you learned.

**Key Indicators of Phishing:**

1. Suspicious email addresses

2.Emails or messages requesting for sensitive information

3.Unusual links or attachments that are used to deliver malware

4.Strange or unusual URLs which leads victims to fake websites

**Actions Taken:**

* Reviewed and applied knowledge to identify phishing: Yes
* Notes: Phishing is a form of online fraud where hackers attempt to get your private information usually by sending false emails or messages in the name of bank or well known websites
* It is basically carried out either by clicking on unknown file or attachment, responding to an unknown or untrusted social media friend requests, using open or free Wi-Fi or clicking on unauthenticated links or ads
* Types of phishing attacks
* Email phishing: The most common type of phishing where users are tricked into clicking unverified spam emails thus revealing their personal information
* Smishing: Here the medium of attack is SMS. SMS texts are sent to victim containing link to fake websites or telling the victim to contact the sender
* Vishing: In this method the attacker calls the victim using modern caller ID spoofing to convince the victim that the call is from trusted source
* Clone phishing: here the attacker copies the email messages that were sent from trusted sources and modifies them by adding links which lead to fake or malicious websites

**6. Device Security Check**

Ensure devices have locks and security software installed.

**Device Security Status:**

* Device 1: Lock Enabled: Yes, Security Software: Yes
* Device 2: Lock Enabled: Yes, Security Software: Yes

**Actions Taken:**

* Enabled Locks/Installed Security Software: Yes
* Notes: on device 1 (Laptop) password protection is enabled and security/antivirus software McAfee is installed with renewed subscription which scans for the pdfs being downloaded to check for any malicious Activity
* On Device 2 (smartphone) password protection is enabled and security/antivirus software google play protect (within play store) is present which scans for new applications being downloaded as well as for any malicious activity in installed applications

**7. Privacy Settings Review**

Review and adjust the privacy settings on your online accounts.

**Privacy Settings Adjusted:**

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

**Actions Taken:**

* Adjusted Privacy Settings: Yes
* Notes: for account 1 (Main account) adjustments have been made in privacy settings such as auto delete enabled for we/app activity older than 18 months, personalized ads have been disabled, other than WhatsApp no other application have any access to my google account, use of verified phone number for improving account security and experience
* For account 2 (recovery account) none of the adjustments have been made till date

**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:**

1. Changed passwords for both the accounts (main account as well as recovery account) and set strong passwords for both of them
2. Installed latest software and operating system updates for both the devices (laptop and smartphone)
3. Enabled 2 factor authentication for one of my accounts (ie: my main account)
4. Educated myself about phishing and the key indicators of phishing
5. Enabled password lock protection system and installed Anti- virus software for both the devices
6. Made privacy adjustments on my main account in order to improve account security and overall experience

**Planned Future Actions:**

1. Always check for latest updates to the software and operating system and install them up to date
2. Enable 2 factor authentication for my recovery account also
3. Never respond to unknown files or attachments sent from untrusted sources and never respond to unknown friend requests on social media platforms
4. Run frequent scans on my smartphone using google play protect in order to scan for any malicious activities on already installed apps as well as apps that will be newly installed
5. Made privacy adjustments on my recovery account as well in order to improve account security