**Personal Cybersecurity Audit and Remediation Plan**

**Learner Name: Monica Akinyi**

**Date:**

**1. Inventory of Digital Assets**

List all your digital devices and online accounts below:

**Digital Devices:**

* Device 1: Laptop, OS Version : windows
* Device 2: smartphone, OS Version: android
* ...

**Online Accounts:**

* Account 1: Gmail account,
* Account 2: Instagram account
* ...

**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: The Gmail account password was being used by other online platforms making it easy for an attacker to get access to the actual account which he could get access to their PII and SPII.
* Account 2: The password was very weak

**Actions Taken:**

* Changed Passwords: Yes/No
* Implemented Password Manager: Yes/No (If yes, which one?)
* **1Password**
* ***It is known for its user-friendly interface and strong security features. It offers apps for various platforms including windows and android for my case and macOS and iOS . 1Password encrypts data locally on the user’s device before syncing it to the cloud , ensuring security.***

**3. Update and Patch**

List any devices or applications that are outdated and need updates.

**Devices/Applications Needing Updates:**

* Device/Application 1:my laptop, web browsers, antivirus software
* Device/Application 2: Smartphone
* ...

**Actions Taken:**

* Updated Devices/Applications: Yes
* Notes:

**Check for Operating System Updates**

Most laptops run on operating systems like Windows, macOS, or Linux. Regularly check for updates through the system's settings or control panel. These updates

often include security patches, bug fixes, and performance improvements.

**Backup Data**:

Before performing updates, it's a good practice to back up important data on the laptop. While updates typically do not affect personal files, data loss can occur due to unforeseen issues during the update process. Regular backups help prevent data loss in such scenarios.

**Update Software Applications**:

In addition to the operating system, regularly update software applications installed on the laptop. Many applications, including web browsers, antivirus software, and productivity tools, receive updates to address security vulnerabilities and improve functionality.

**Enable Automatic Updates**:

To ensure timely updates, enable automatic updates for the operating system and software applications whenever possible. This way, updates are installed automatically in the background without requiring manual intervention.

**Restart the Laptop**

After installing updates, restart the laptop to apply the changes fully. Some updates may require a restart to take effect, especially for system-level updates.

**Monitor Update Status**

During the update process, monitor the progress to ensure updates are successfully installed without errors. If any issues arise, troubleshoot them promptly to prevent potential security risks or performance problems.

**Update Firmware and Drivers**

In addition to software updates, periodically check for firmware and driver updates for hardware components such as the motherboard, graphics card, and network adapter. These updates can improve stability, compatibility, and security.

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

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

**Accounts Supporting 2FA:**

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

**Actions Taken:**

* Enabled 2FA on Accounts: Yes
* Notes:

**Enable 2 Factor Authentication**

First and foremost, enable 2FA wherever it's available. This typically involves logging into an account and setting up an additional authentication method, such as receiving a code via SMS, using a mobile authenticator app (like Google Authenticator or Authy), or using hardware tokens.

**Use App-Based Authentication**:

Whenever possible, opt for app-based authentication methods over SMS-based ones. App-based authentication is generally more secure as it's not vulnerable to SIM swapping attacks or interception of SMS messages.

**Secure Recovery Options**

Make sure that the recovery options for 2FA are secure. This could involve setting up backup codes, providing alternate email addresses or phone numbers, or using other trusted devices for recovery purposes.

**Protect Physical Tokens**

If using hardware tokens (e.g., YubiKeys), ensure they are stored securely and are not easily accessible to unauthorized individuals. Treat them like physical keys to your accounts.

**Monitor Authentication Attempts**

Implement monitoring systems to track authentication attempts, especially failed attempts or suspicious activity. This can help identify and respond to potential security threats in a timely manner.

**Stay Informed**

Stay informed about security best practices and emerging threats related to 2FA. Subscribe to security newsletters, follow reputable cybersecurity blogs, and participate in relevant forums or communities to stay updated on the latest developments in 2FA security.

**5. Educate Yourself on Phishing**

Summarize key indicators of phishing attempts you learned.

**Key Indicators of Phishing:**

**Mismatched URLs**

Phishing emails often contain links that lead to deceptive websites with URLs that closely resemble legitimate ones but may have misspellings or extra characters.

**Urgent or Threatening Language**

Phishing emails often create a sense of urgency or fear to prompt immediate action, such as claiming that an account will be suspended unless action is taken.

**Request for Personal Information**

Phishing emails commonly request sensitive information like passwords, credit card numbers, or account details, often posing as legitimate organizations.

**Suspicious Attachments/** **Unsolicited Links**

Phishing emails may contain attachments or links that, when clicked, install malware or viruses onto the recipient's device.

**Generic Greetings**

Phishing emails often use generic greetings like "Dear Sir/Madam" instead of addressing the recipient by name.

**Unsolicited Requests**

Phishing emails typically arrive unexpectedly, without prior interaction or relationship with the sender.

**Poor Spelling and Grammar**

Phishing emails often contain spelling and grammatical errors, suggesting a lack of professionalism or attention to detail.

**Unexpected Email Addresses**

Phishing emails may come from unfamiliar or suspicious email addresses that do not match the sender's purported identity.

**Spoofed Sender Information**

Phishing emails may spoof the sender's name or email address to appear as though they are from a trusted source.

**Requests for Login Credentials**

Phishing emails often request login credentials for online accounts under the guise of security measures or account verification.

**Actions Taken:**

* Reviewed and applied knowledge to identify phishing: Yes
* Notes:

**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:

**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:
* **Choose a Reputable Security Software**: Select a trusted security software solution from a reputable provider. Look for features such as antivirus, anti-malware, firewall, and real-time threat detection.
* **Install and Update Regularly**: Install the security software on all devices that need protection, including computers, smartphones, and tablets. Ensure that the software is updated regularly to guard against the latest threats.
* **Enable Real-Time Protection**: Activate real-time protection features within the security software to continuously monitor for threats and prevent malware infections in real-time.
* **Perform Regular Scans**: Schedule regular system scans to detect and remove any malware or suspicious files that may have evaded real-time protection.
* **Enable Firewall Protection**: Enable the firewall feature provided by the security software to monitor and control incoming and outgoing network traffic, thereby preventing unauthorized access to your device.
* **Configure Security Settings**: Review and configure the security settings of the software according to your preferences and security requirements. Adjust settings related to threat detection sensitivity, scanning schedules, and quarantine actions.
* **Enable Automatic Updates**: Enable automatic updates for the security software to ensure that it stays up-to-date with the latest virus definitions, security patches, and software improvements.
* **Keep Operating System and Software Updated**: In addition to security software updates, regularly update the operating system and other software applications on your devices to patch vulnerabilities and improve overall security.
* **Use Strong Passwords**: Protect access to the security software with a strong, unique password to prevent unauthorized changes or disabling of security features.
* **Exercise Caution Online**: Even with security software installed, practice safe browsing habits and exercise caution when interacting with email attachments, links, and downloads from unknown or suspicious sources.
* **Backup Important Data**: Implement a regular backup strategy to safeguard important data against data loss due to malware infections, hardware failures, or other unforeseen events.
* **Educate Users**: If securing devices within an organization, provide training and education to users on best practices for using security software effectively and recognizing potential security threats.

**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:**

***Continuous Monitoring and Assessment***

***Enhanced Network Security Measures:***

***Advanced Threat Detection Technologies***

***Employee Awareness Programs***

***Integration of Security Automation:***

***Regular Security Audits and Assessments***

**Planned Future Actions:**