Personal Cybersecurity Audit and Remediation Plan

Learner Name: Mann Kaniyawala

Date: 22nd June, 2024

1. Inventory of Digital Assets

List all your digital devices and online accounts below:

Digital Devices:

- Device 1: **Smartphone**, Apple iPhone 14 Pro, iOS 17.5.1
- Device 2: **Laptop**, Dell XPS 15, Windows 11
- Device 3: **Tablet PC**, Apple iPad Pro 3rd Gen, iOS 17.5.1

Online Accounts:

- Account 1: Email, **Gmail** (Google)
- Account 2: Email, **Outlook** (Microsoft)
- Account 3: Social Media, **Instagram** (Meta)
- Account 4: Social Media, **Facebook** (Meta)
- Account 5: Social Media, **Reddit** (Advance Publications)

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: Facebook
- Account 2: Reddit

Actions Taken:

- Changed Passwords: **Yes** (Started regularly changing passwords of all accounts more often)
- Implemented Password Manager: **Yes** (**Google Password Manager**)

3. Update and Patch

List any devices or applications that are outdated and need updates.

Devices/Applications Needing Updates:

- Application 1: Duolingo
- Application 2: Spotify
- Application 3: Google Maps

Actions Taken:

- Updated Devices/Applications: **Yes**
- Notes: Had updates pending for the above-mentioned apps. The new updates ensure better working and efficiency of the app. Also fixing minor bugs makes them runs smoothly.

4. Two-Factor Authentication (2FA)

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

Accounts Supporting 2FA:

- Gmail: 2FA Enabled: **Yes**
- Outlook: 2FA Enabled: **Yes**
- Reddit:2FA Enabled: **No**
- Instagram:2FA Enabled: **Yes**
- Facebook:2FA Enabled: **No**

Actions Taken:

- Enabled 2FA on Accounts: **Yes**
- Notes: Enabling 2-Factor Authorization creates an extra layer of security for the accounts protecting user data, activity and some information(personal & application based.)

5. Educate Yourself on Phishing

Summarize key indicators of phishing attempts you learned.

Key Indicators of Phishing:

1. Emails, texts from untrusted/random accounts with suspicious links.
2. Links ask for your personal and financial information.

3. Formatting and grammar of email is not proper.

Actions Taken:

- Reviewed and applied knowledge to identify phishing: **Yes**
- Notes: Not trusting random emails, inspecting links and using anti-phishing tools and firewalls etc.

6. Device Security Check

Ensure devices have locks and security software installed.

Device Security Status:

- Phone: Lock Enabled: **Yes**, Security Software: **No**
- Laptop: Lock Enabled: **Yes**, Security Software: **Yes**
- Tablet PC: Lock Enabled: **Yes**, Security Software: **No**

Actions Taken:

- Enabled Locks/Installed Security Software: **Yes**
- Notes: By choosing a reputable software and installing it on your device followed by configuring it to suit your device and make the most out of the software.

7. Privacy Settings Review

Review and adjust the privacy settings on your online accounts.

Privacy Settings Adjusted:

- Instagram: Adjustments Made: **Yes**
- Facebook: Adjustments Made: **Yes**
- Reddit: Adjustments Made: **No**

Actions Taken:

- Adjusted Privacy Settings: Yes
- Notes: Making personal information protected and hiding your photos/videos from anyone other than people you know. Enabling 2-Factor Authorization on the account.

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:

- Installing security software
- Updating outdated apps
- Enhancing security on certain apps and websites
- Using a password manager

Planned Future Actions:

- Improving the security of internet provider.
- Implement additional threat detection tools such as intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Store valuable data by taking backups on external hard-drives.