**Assessment of Current Practices**

**Password Management**: Use of strong, unique passwords for different accounts.

**Two-Factor Authentication (2FA)**: Implementation of 2FA for critical accounts.

**Software Updates**: Regular updates of operating systems and applications.

**Antivirus Software**: Installation and regular updates of antivirus programs.

**Backup Practices**: Regular backups of important data to secure locations.

**Secure Browsing**: Use of secure browsers and avoiding suspicious links.

Areas of Improvement

Password Strength: Ensure all passwords are complex and stored securely using a password manager.

2FA Coverage: Extend 2FA to all possible accounts, not just critical ones.

Update Frequency: Increase the frequency of checking for and installing updates.

Phishing Awareness: Improve knowledge and recognition of phishing attempts.

Network Security: Use VPNs on public Wi-Fi networks and secure home networks.

Data Encryption: Encrypt sensitive data stored on devices and cloud services.

Risk Analysis

Weak Passwords: High severity and likelihood. Easily mitigated by using a password manager.

Limited 2FA Usage: Medium severity and likelihood. Addressed by expanding 2FA coverage.

Infrequent Software Updates: High severity and medium likelihood. Mitigated by scheduling regular update checks.

Phishing Attacks: High severity and high likelihood. Reduced by increased awareness and training.

Unsecured Networks: Medium severity and likelihood. Addressed by using VPNs and securing networks.

Unencrypted Data: Medium severity and medium likelihood. Mitigated by implementing data encryption.

Personal Cyber Hygiene Improvement Plan

Strengthening Password Management

Implement a password manager to generate and store complex passwords.

Regularly update passwords and avoid using the same password for multiple accounts.

Expanding Two-Factor Authentication

Enable 2FA on all accounts that support it, especially those with sensitive information.

Use authentication apps or hardware tokens for added security.

Regular Software Updates

Schedule regular checks for operating system and application updates.

Enable automatic updates where possible.

Increasing Phishing Awareness

Participate in cybersecurity awareness training and stay informed about common phishing tactics.

Be cautious with emails and links from unknown sources.

Securing Networks

Use VPNs when accessing public Wi-Fi networks.

Ensure home networks are secured with strong passwords and updated firmware.

Implementing Data Encryption

Encrypt sensitive data stored on devices and cloud services.

Use encrypted communication channels for transmitting sensitive information.

Using Antivirus and Anti-Malware Software

Install reputable antivirus and anti-malware software on your devices. Schedule regular scans to detect and remove potential threats.

Enable real-time protection features to continuously monitor your system for malicious activity. This proactive approach helps prevent infections before they cause damage.

Backup Security

Encrypt backups to protect them from unauthorized access. Ensure that backup solutions also include redundancy to prevent data loss.

Education and Information

Stay informed about the latest cyber threats and best practices by following reputable sources like cybersecurity blogs, news outlets, and official advisories.

Plan for Periodic Re-evaluation of Your Cyber Hygiene

Establishing a Baseline

Set a schedule for regular re-evaluation of your cyber hygiene.

Key Areas for Re-evaluation

Focusing on these key areas during each re-evaluation: access controls, software updates, data protection and incident response

Training and Awareness