# Employee Feedback

### Feedback and Action Plan for Improved Digital Hygiene

Hello there! It's fantastic to see your commitment to improving your cybersecurity practices. You're already on a solid path with several key habits, such as using a password manager and multi-factor authentication. Let's build on these strengths and tackle some areas for improvement to boost your security score.

## **What You're Doing Well**

- **Secure Password Storage:** Using a password manager is a great way to keep unique and complex passwords secure.
- **Consistent Use of MFA:** Excellent job in implementing an extra layer of security for your accounts.
- **Prompt Software Updates:** Quickly installing updates helps to protect your devices from vulnerabilities.
- **Device Usage Policies:** Adhering to policies ensures compliance and security.
- **Using Encrypted Channels:** This helps keep your communications confidential.
- **Incident Reporting:** Knowing how and feeling comfortable reporting issues is crucial for a responsive security posture.

## **Areas to Improve**

#### **Password Practices**

- **Action Step:** Start generating unique passwords for each account. Consider using your password manager's password generator feature.

#### **Device Security**

- **Action Step:** Develop a habit of locking your devices whenever you step away, even for a short moment. Perhaps set a short lock screen timer to help automate this.

#### **Phishing Awareness**

- **Action Step:** Make it a routine to hover over email links to see the actual URL before clicking and verify sender information.

#### **Security Training**

- **Action Step:** Enroll in upcoming security training sessions to stay updated on the latest threats and defenses.

#### **Email Verification**

- **Action Step:** Take a moment to verify the legitimacy of emails, especially those prompting action, before clicking on any links.

#### **Suspicious Emails**

- **Action Step:** Report any suspicious emails to your IT department. This helps in fortifying the organization's security defenses.

#### **Remote Work Practices**

- **Action Step:** Use a VPN whenever accessing work resources from remote locations to encrypt your internet traffic.
- **Public Wi-Fi Usage:** Prefer using a personal hotspot instead of public Wi-Fi when possible.

#### **Shared Device Policy**

- **Action Step:** Make it a point to keep work devices personal and refrain from sharing them to maintain data integrity.

#### **Training Exercises**

- **Action Step:** Actively sign up and participate in security training exercises to enhance your practical knowledge.

**Action Plan**

#### **Immediate (0–30 Days)**

- **Watch Out for Suspicious Activities:** Refrain from clicking on suspicious links and attachments immediately.
- **Update Passwords:** Start updating passwords, focusing on uniqueness and complexity.
- **Device Locking:** Integrate locking practices into your daily routine.

#### **Short-Term (60–90 Days)**

- **Enroll in Training:** Make time to attend cybersecurity training programs. These sessions are designed to heighten your awareness and sharpen your skills.
- **Social Engineering Awareness:** Dedicate time weekly to practice identifying phishing attempts and other social engineering tactics through available simulation exercises.

Remember, these changes, though procedural, contribute significantly to a stronger, more secure work environment. Keep up the great work, and always feel free to reach out with any questions or for further

guidance. You're on your way to becoming a cybersecurity pro! Keep the momentum going; you've got this!
■