Employee Feedback

Feedback and Action Plan for Improving Digital Hygiene

Hello! It's great that you're taking steps to improve your digital hygiene. By focusing on these areas, you can significantly enhance your cybersecurity awareness and practices. Let's tackle this together!

What You're Doing Well:

While there isn't a specific area highlighted, having moderate practices in all areas means you're already aware of many essential aspects of cybersecurity. This is a promising foundation for improvement!

Areas to Improve & Actionable Steps

1. Password Management:

- **Immediate:**
- Start using a password manager to create and store strong, unique passwords for each account. This significantly reduces the risk of breaches if one account is compromised.
- **Short-Term:**
- Go through your existing accounts and update them with stronger, unique passwords.

2. Multi-Factor Authentication (MFA):

- **Immediate:**
- Enable MFA on all accounts that offer it. This extra layer of security can prevent unauthorized access even if your password is compromised.

3. Device Security:

- **Immediate:**
- Get into the habit of locking your computer and devices when stepping away, even for a short time.
- Regularly check for and install updates for your operating system and applications to protect against vulnerabilities.
- **Short-Term:**

- Explore the use of VPNs for securing your internet connection, especially when accessing sensitive information remotely.

4. Phishing Awareness:

- **Immediate:**
- Double-check sender addresses on emails, and if anything seems off, do not click on links or open attachments.
- Report any suspicious emails to your IT/security department to help them keep everyone safe.
- **Short-Term:**
- Engage in available phishing and cybersecurity training sessions. These will help you learn to recognize and avoid social engineering attempts.

5. Secure Communication:

- **Short-Term:**
- Begin using encrypted communication channels for sensitive discussions. This ensures that your work conversations remain confidential and protected.

6. Avoiding Public Wi-Fi:

- **Immediate:**
- Whenever possible, avoid conducting work transactions over public Wi-Fi. If necessary, use a VPN to secure your connection.

7. Reporting and Training:

- **Immediate:**
- Familiarize yourself with the process for reporting cybersecurity incidents, and feel empowered to report any mistakes or security concerns without hesitation.
- **Short-Term:**
- Advocate for and participate in any organizational cyber exercises, such as simulated phishing tests.

8. Organizational Culture:

- Reflect on and communicate with your organization about enhancing cybersecurity training, ensuring everyone feels supported and knowledgeable in maintaining security.

Friendly Motivation:

You're on the right path! Each step you take not only strengthens your security resilience but also contributes to a safer digital environment for everyone. Keep pushing forward, and feel confident that you're making tangible improvements in your cyber safety practices. Remember, small changes can lead to significant impacts!

Feel free to reach out if you need any more tips or guidance. You're doing great, and every effort counts!