Employee Feedback

Absolutely, enhancing your digital hygiene is a great step toward securing both personal and organizational information. Let's focus on the areas that require improvement while reinforcing the practices you're already excelling in. Here's a structured and actionable plan to help you enhance your cybersecurity posture:

What You're Doing Well

First, let's celebrate where you're shining:

- **Unique Passwords and Secure Storage**: You're doing fantastic here! Keep using strong, unique passwords for all your accounts and continue to store them securely.
- **Multi-Factor Authentication (MFA)**: Your excellent use of MFA adds a crucial layer of security.
- **Device and Communication Security**: Consistently locking devices and using encrypted channels are excellent practices that protect sensitive information.
- **Phishing Awareness and VPN Use**: Your ability to recognize phishing attempts and use of a VPN showcases strong cybersecurity awareness.

Areas to Improve

1. **Phishing Attack Training and Awareness**

- **Immediate Action**: Make time to watch some online resources or tutorials about phishing to boost your awareness. Begin by viewing examples of phishing emails to hone your detection skills.
- **Short-Term Goal**: Enroll in any available cybersecurity training sessions that your organization offers. The more you recognize phishing tactics, the more intuitive avoiding them will become.

2. **Report Suspicious Activities**

- **Immediate Action**: Familiarize yourself with the process of reporting suspicious emails or activities to your IT or security team. Knowing who to contact can save valuable time.
- **Motivation**: Understand that your vigilance can protect not just your data but the entire organization's security posture.

3. **Device and Software Updates**

• **Immediate Action**: Set reminders to regularly check for updates for your operating system and all applications, including security patches. Often, these updates fix vulnerabilities.

• **Short-Term Goal**: Allocate some time weekly to review updates and perform system restarts to ensure they are applied properly.

4. **Using Work Devices Appropriately**

• **Immediate Action**: Avoid using personal USB drives or installing unauthorized software on work devices. This prevents inadvertent malware infections.

• **Plan**: If you need to use external storage devices, make sure they are scanned for viruses before use.

5. **Cybersecurity Culture and Reporting Comfort**

• **Building Comfort**: Know that mistakes happen, but reporting them leads to resolution. Create a personal goal to bring up any security-related queries in team meetings to build confidence.

• **Organizational Effort**: You might consider providing feedback to your organization about your desire for more comprehensive cybersecurity training and better communication channels for incident reporting. A collective effort improves overall security.

Conclusion

Your score shows there is room for improvement, but your current practices provide a strong foundation. Remember, consistent, small steps can lead to big improvements in digital security. Stay motivated, keep learning, and don't hesitate to communicate with your team or IT department when needed.

By implementing the actionable steps above, you are not only protecting yourself but also contributing to a safer online environment for your organization. Keep up the great work, and continue to build on your cybersecurity skills!