Employee Feedback

Certainly! Here's some structured and actionable feedback to help improve your digital hygiene:

Hi [Employee's Name],

It looks like you're on your way to improving your digital security, and that's fantastic! Let’s tackle those remaining challenges so you can protect yourself and your organization even better. Remember, every step you take enhances your cybersecurity posture. Let’s dive in.

What You're Doing Well

While it seems there are no specific areas marked as 'doing well' yet, recognize that progress in each 'Moderate practice' area is a solid foundation to build upon. You're already aware of key practices, and that awareness is your first line of defense.

Immediate Action Plan (0–30 Days)

1. **Avoid Suspicious Links**: If something seems off—trust your instincts! Always verify links and attachments before clicking, especially in unexpected emails. Hover over links to see if URLs look authentic, and don’t hesitate to reach out to IT if you're unsure.

2. **Strong, Unique Passwords**: Consider using a password manager to generate and store unique passwords for each of your accounts. This will take a significant load off your memory and enhance security.

3. **Enable Multi-Factor Authentication (MFA)**: Whenever available, turn on MFA for your accounts. This adds an extra layer of security by requiring a second form of verification.

4. **Stay Updated**: Regularly check for software updates on your devices. These updates often contain critical security patches, so prompt installation is crucial. Restarting your devices ensures updates are fully applied.

Short-Term Action Plan (60–90 Days)

1. **Participate in Cybersecurity Training**: Engage in any cybersecurity training opportunities provided by your organization. These sessions are designed to keep you informed and prepared against cyber threats like phishing.

2. **Identify and Avoid Social Engineering Attempts**: With practice, you'll become adept at spotting email scams and other social engineering attempts. Consider joining simulated exercises—phishing tests can be

both challenging and fun!

3. **Limit Use of Personal Devices for Work**: Keep work tasks on work devices only, and discourage the use of personal USB drives or unauthorized software on them. This minimizes exposure to malware and other vulnerabilities.

Friendly Reminder

Your efforts not only protect your data but also safeguard our company's information and resources. If you ever make a mistake or notice something suspicious, it's important to report it immediately—your transparency can prevent larger issues. Remember, cybersecurity is a shared responsibility!

Stay Encouraged!

You care about improving, and that's the most important part. Each improvement you make reduces potential risks significantly. Keep building on this progress, and don't hesitate to ask any questions or for help.

Together, we can create a safer digital environment for everyone. Thanks for your effort and dedication!

Best regards,

[Your Name]

Cybersecurity Advisor

Remember, small consistent improvements create the biggest impacts over time. Keep up the good work!