Employee Feedback

■ **Great Job on Your Cyber Hygiene Efforts!**

You've made a commendable effort to maintain a secure digital workspace, and your commitment is clearly reflected in your score and practices. Let's celebrate your strengths and look at ways to enhance your cybersecurity skills further!

■ What You're Doing Well - **Unique Passwords & Secure Storage**: You're setting the standard by using unique passwords and storing them securely. Keep it up! ■ - **Multi-Factor Authentication (MFA)**: Excellent use of MFA adds an extra layer of security. This is a strong defense against cyber threats! ■ - **Device Security**: Locking your devices when unattended shows great awareness. You're protecting your data like a pro! ■ - **Phishing Awareness**: Your ability to recognize and report phishing emails is impressive. This protects not only you but your entire organization. ■■ - **Cybersecurity Training Participation**: Staying informed with training reflects your proactive approach to security. Well done! ■ - **Careful with Email Attachments**: Your vigilance with email sender verification helps avoid unnecessary risks. ■ - **Device Management**: Regular updates and avoiding unauthorized software demonstrate responsibility and caution. ■ - **Using Secure Connections**: Utilizing a VPN and secure connections while working remotely shows your foresight and dedication to safety. ■ - **Awareness About Public Wi-Fi**: Avoiding public Wi-Fi for work tasks is a smart move to keep your data secure. ■ - **Maintaining Device Privacy**: Ensuring exclusive use of work devices for yourself is excellent practice. ■

■■ Areas to Improve - None! You're doing great across the board! ■

■ Potential Risks - Staying vigilant about phishing emails is crucial for protecting sensitive information. - Continuously improve password habits to ensure you stay ahead of potential security threats. - Regular updates are the best defense against malware and cyber-attacks.

■■ Action Plan ### ■ Immediate - **Be Thorough with Emails**: Keep verifying email senders and think twice before clicking any links. - **Strengthen Passwords**: Continue using complex passwords and pair them with MFA whenever possible. - **Update Regularly**: Maintain the routine of updating your work devices frequently to close any security loopholes.

■ Next 2–3 Months - **Expand Your Training**: Dive deeper into cybersecurity training sessions to stay informed about emerging threats. - **Enhance Social Engineering Awareness**: Brush up on spotting social engineering tactics, including fake tech support.

Your proactive approach and diligence are truly commendable. By following the action plan, you'll become an even more cyber-safe employee, setting a stellar example for others. Keep up the excellent work! ■