Employee Feedback

# ■ Cyber Hygiene Feedback ■

## ■ Great Start: You're Taking Steps Forward! It's fantastic to see your dedication to improving your cyber hygiene. While there aren't specific areas listed where you're excelling yet, you're already on the path to becoming more cyber-saavy by acknowledging the practices that need strengthening. Keep pushing forward, and you'll see progress!

## ■■ Areas to Improve

Here are some areas where a little effort can make a big difference:

### Password Management ■ - **Use Unique Passwords**: Ensure every account has a different password to reduce the risk if one gets compromised. - **Store Passwords Securely**: Consider using a password manager to keep track of them safely.

### Security Practices ■ - **Enable MFA**: Two-factor authentication adds an extra layer of protection. Turn it on wherever possible.

### Device Security ■ - **Lock Your Devices**: Always lock devices when away. It's a simple but effective security measure. - **Regular Updates**: Keep your operating system and apps updated to guard against security vulnerabilities.

### Email and Phishing Awareness ■ - **Phishing Detection**: Enhance your ability to spot phishing emails by closely examining sender details and suspicious links. - **Report to IT**: Immediately flag any suspicious emails or activities to your IT/security team.

### Secure Connectivity ■ - **VPN Usage**: Use a VPN when accessing work systems remotely, especially over public Wi-Fi. - **Encrypted Channels**: Ensure sensitive work conversations use secure, encrypted communication tools.

### Organizational Confidence ■ - **Training Participation**: Engage in available training to boost your knowledge and preparedness. - **Incident Reporting**: Build confidence in recognizing and reporting any security issues or potential breaches.

## ■ Potential Risks

Your current practices leave some room for cyber threats, including: - ■ **Phishing Attacks**: Potential success due to lack of detection skills. - **Password Weaknesses**: Risk of unauthorized access from password-related issues. - ■ **System Vulnerabilities**: Unpatched devices can be targeted by malware.

## ■■ Action Plan for Improvement

### ■ Immediate Actions - **Vigilance with Emails**: Double-check sender information and resist clicking on any uncertain links. - **Build Better Passwords**: Start using a combination of letters, numbers, and symbols for unique passwords across accounts. - **Update Routine**: Make it a habit to install updates and restart your devices for optimal security.

### ■ Upcoming Goals (Next 2–3 Months) - **Cyber Training**: Increase your cybersecurity skills by participating in training and simulated exercises offered by your organization. - **Recognize Social Engineering**: Sharpen your awareness of common tactics like fake tech support scams.

### ■ Keep Going! We're here to help you grow confident in securing your digital workspace. Remember, every small change you make contributes to a much safer environment for both you and your organization. Keep up the good work! ■