Employee Feedback

Cyber Hygiene Score

39.71%

Needs Improvement: You're making progress, but there are significant gaps.

Introduction

Your current cybersecurity hygiene is considered weak, indicating there is room for improvement. Good cyber habits are vital for both your safety and the security of our organization. By enhancing your cybersecurity practices, you help protect sensitive information from threats and minimize the risk of breaches.

What You're Doing Well

Here are some cybersecurity practices you are already following effectively:

- **Locking Devices:** You lock your computer and devices when leaving them unattended. This prevents unauthorized access to your work and personal information.
- **Phishing Awareness:** You would recognize a phishing email, which helps you avoid scams and potential data breaches.
- **Phishing Training:** You have received training on phishing attacks. This education is crucial in recognizing and mitigating sophisticated email threats.
- **Use of VPNs:** You use a VPN or secured connection when working remotely, ensuring that your data is protected from eavesdroppers in insecure networks.

Areas to Improve

Here are some areas where improvement is needed:

Password & Access Management

- **Unique Passwords:** Ensure you use unique passwords for different accounts. This prevents a single data breach from compromising all your accounts.
- **Secure Password Storage:** It’s important to securely store your passwords. Consider using a password manager to keep them organized and protected.

- **Multi-Factor Authentication (MFA):** Use MFA whenever available. It adds an extra layer of security, making it harder for attackers to access your accounts.

Phishing Awareness & Email Security

- **Verify Sender Addresses:** Always verify sender addresses before clicking links or opening attachments. This helps avoid falling victim to phishing attacks.
- **Report Suspicious Emails:** Make sure to report any suspicious emails to IT/security. Prompt reporting can help prevent potential breaches.

Device & Data Security

- **Regular Updates:** Regularly update your work device’s operating system, apps, and security patches. This keeps you protected against known vulnerabilities.
- **Avoid Unauthorized Software:** Don’t use personal USB drives or unauthorized software on work devices to prevent malware infections.
- **Encrypted Communication:** Use encrypted channels for sensitive work discussions to protect your data from being intercepted.

Remote Work & Public Network Security

- **Avoid Public Wi-Fi:** Steer clear of using public Wi-Fi for work tasks to prevent exposure to potential attacks on unsecured networks.
- **Device Sharing:** Ensure that family members or friends do not use your work devices to maintain control over access and usage.

Incident Reporting & Cybersecurity Culture

- **Incident Reporting:** Learn how to report a cybersecurity incident promptly, ensuring quick action and resolution.
- **Simulated Exercises:** Participate in simulated cybersecurity exercises like phishing tests to improve your readiness for real threats.
- **Comfort in Reporting Errors:** Feel confident reporting mistakes or security issues to IT/security to contribute to a proactive and supportive security culture.

Potential Risks and Risk Scenarios

Here are some risks related to current gaps:

- **Password Reuse:** If you reuse passwords, a breach on one site could expose your other accounts.
- **Phishing Vulnerability:** Opening suspicious links could lead to malware infection or data theft.

- **Device Exposure:** Not updating your device regularly increases vulnerability to known exploits.

Personal Cyber Hygiene Action Plan

Immediate (0–30 Days)

Quick wins and critical fixes:

- Create unique passwords for your most sensitive accounts.
- Set up multi-factor authentication (MFA) where available.
- Begin using a password manager to securely store credentials.
- Report any suspicious emails to IT/security.

Short-Term (60–90 Days)

Mid-term improvements:

- Learn how to verify email authenticity by checking sender addresses.
- Regularly update your device’s software and apps.
- Avoid using public Wi-Fi for work tasks or use a VPN if necessary.

Medium-Term (3–6 Months)

Long-term habit building:

- Organize a routine schedule for system and application updates.
- Practice recognizing newer phishing techniques through refresher courses.
- Participate in cybersecurity exercises to gain practical experience.
- Encourage open dialogue about cybersecurity concerns within your team.

Conclusion

Keep improving your cybersecurity practices. Small actions — like updating your passwords or learning to spot phishing emails — can have a big impact. I encourage you to review your cyber hygiene again in 6–12 months to track your progress and continue strengthening your security habits. Remember, we’re here to support you every step of the way!