Employee Feedback

Cyber Hygiene Feedback Report

Cyber Hygiene Score

39.71%

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

Introduction

You currently have a weak level of cybersecurity hygiene, based on your self-assessment score. It's important to focus on improving your cybersecurity habits to better protect both yourself and our organization. Strong cybersecurity practices help safeguard sensitive information and prevent potential security breaches. Don't worry, though—you're in the right place to learn how to strengthen your cyber defenses!

What You're Doing Well

Great job on these aspects of cybersecurity! Keep it up!

- **Locking Devices:** You lock your computer and devices when leaving them unattended. This prevents unauthorized access, ensuring your work and personal data remain secure.
- **Phishing Awareness:** You would recognize a phishing email, which helps prevent identity theft and unauthorized access.
- **Security Training:** You've received cybersecurity training on phishing attacks. Knowledge is power and keeps you one step ahead of potential threats.
- **Secure Connections:** You use a VPN or secured connection when working remotely, safeguarding data from internet threats on public networks.

Areas to Improve

Password & Access Management

- **Unique Passwords:** Ensure you use unique passwords for different accounts. This prevents a single data breach from compromising multiple accounts.
- **Secure Password Storage:** Consider using a password manager, which can safely store and organize your passwords.

• **Multi-Factor Authentication (MFA):** Activate MFA wherever possible. It adds an extra layer of security beyond just passwords.

Phishing Awareness & Email Security

• **Verify Sender Addresses:** Begin verifying sender addresses before clicking links or opening attachments. This helps prevent falling victim to malicious links.

• **Report Suspicious Emails:** Report suspicious emails to IT/security promptly to prevent potential breaches.

Device & Data Security

• **Regular Updates:** Regularly update your work device, including the OS, apps, and security patches, to shield against vulnerabilities.

• **Avoid Unauthorized Devices/Software:** Do not use personal USB drives or unauthorized software on work devices as they can introduce malware.

• **Encryption:** Use encrypted communication channels when discussing sensitive work information, ensuring confidentiality.

Remote Work & Public Network Security

• **Avoid Public Wi-Fi:** Refrain from using public Wi-Fi for work tasks as these networks are often insecure.

• **Restrict Device Access:** Ensure that only you use your work devices to prevent unintentional security breaches by others.

Incident Reporting & Cybersecurity Culture

• **Incident Reporting:** Familiarize yourself with the cybersecurity incident reporting process to respond quickly in case of an issue.

• **Participate in Exercises:** Engage in simulated cybersecurity exercises to practice and improve response tactics.

• **Open Communication:** Feel comfortable reporting mistakes to IT/security. Prompt reporting can prevent escalation.

Potential Risks and Risk Scenarios

• **Password Reuse:** If you reuse the same password everywhere, a data breach on one site could expose all your accounts.

• **Phishing Exposure:** Clicking on unverified links can lead to malware infections or unauthorized access.

- **Outdated Software Vulnerabilities:** Not updating software can leave devices susceptible to known security threats.
- **Public Network Risks:** Using public Wi-Fi can allow attackers to intercept sensitive information.

Personal Cyber Hygiene Action Plan

Immediate (0–30 Days)

Quick wins and critical fixes:

- Start by using a password manager to create and store unique passwords.
- Activate MFA on all accounts that offer it.
- Begin verifying sender addresses in emails and report any suspicious activity to IT/security.
- Avoid public Wi-Fi for work-related tasks immediately.

Short-Term (60–90 Days)

Mid-term improvements that may need a bit more time or learning:

- Schedule regular updates for your operating system and software.
- Participate in our next scheduled phishing exercise.
- Learn how to use encrypted communication tools for sensitive discussions.

Medium-Term (3–6 Months)

Longer-term changes to build sustainable habits:

- Continually update and improve your password manager as needed.
- Engage actively in cybersecurity training sessions to broaden your knowledge.
- Regularly review and revise cybersecurity practices to adapt to emerging threats.

Conclusion

Keep striving to improve your cybersecurity practices. Remember, even small actions—like updating passwords or learning to spot phishing attempts—can have a significant impact. Consider reviewing your cyber hygiene again in 6–12 months to see your progress. Your journey to better cybersecurity is also a crucial part of strengthening our organization's defenses. We're here to support you along the way!