Employee Feedback

Cyber Hygiene Score

79.41%

Good Start: You're doing well, but there's room for improvement.

Introduction

Your current cybersecurity hygiene is quite strong, demonstrating a solid foundation of good habits that protect both you and our organization. Maintaining good cybersecurity practices is crucial to safeguarding personal information and preventing unauthorized access to company data. This score indicates you're on the right track, but there's always room for improvement to stay ahead of cyber threats.

What You're Doing Well

- **Password Storage:** It seems you store your passwords securely, which is vital in keeping unauthorized users from accessing your accounts.
- **Multi-Factor Authentication (MFA):** Using MFA adds an extra layer of security, making it significantly harder for attackers to gain access.
- **Device Security:** Locking your devices when unattended protects sensitive information from being accessed by others.
- **Email Vigilance:** Recognizing a phishing email is crucial in preventing breaches. You seem capable of identifying suspicious emails, reducing the risk of malware or data theft.
- **Link Verification:** Checking sender addresses and verifying links help prevent falling for phishing scams.
- **Report Suspicious Activities:** Reporting questionable emails to IT/security helps keep the organization secure by proactively addressing potential threats.
- **Regular Updates:** Keeping your operating system and apps updated ensures you have the latest security patches and protections in place.

Areas to Improve

Password & Access Management

- **Unique Passwords:** It’s important to use unique passwords for each account to prevent a breach from affecting multiple accounts simultaneously.

Phishing Awareness & Email Security

- **Cybersecurity Training:** Engaging in training on phishing attacks will strengthen your ability to detect and avoid phishing attempts.

Incident Reporting & Cybersecurity Culture

- **Simulated Exercises:** Participating in exercises such as phishing tests can help you recognize threats in a risk-free environment and prepare you for real scenarios.

Potential Risks and Risk Scenarios

- Using the same password everywhere increases the risk of widespread account compromise if even one account is breached.
- Without adequate phishing training, you might inadvertently click on malicious links, risking exposure of sensitive data.

Personal Cyber Hygiene Action Plan

Immediate (0–30 Days)

Quick wins and critical fixes:

- Start using strong, unique passwords for every account. Consider using a passphrase or a password manager if you haven't already.
- Ensure multi-factor authentication is enabled wherever possible.
- Be cautious with suspicious emails — avoid clicking unsolicited links or attachments.
- Update all software and operating systems immediately to patch security vulnerabilities.
- Regularly restart your computer to ensure updates are properly applied.

Short-Term (60–90 Days)

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

- Enroll in and complete a cybersecurity awareness training program.
- Improve your ability to identify phishing and social engineering attempts by reviewing the organization's phishing guidelines.
- Explore different password manager options to streamline your password management securely.
- Set your devices to auto-lock after a short period of inactivity to enhance security.

Medium-Term (3–6 Months)

Longer-term changes to build sustainable habits:

- Create a personal routine to check for and apply monthly software updates without fail.
- Delve into and adjust privacy settings across your digital services for enhanced protection.
- Develop secure habits for remote work, such as using VPNs and avoiding public Wi-Fi, to keep your data safe while traveling or working outside the office.

Conclusion

Keep pushing forward with your cybersecurity practices. Remember that small actions, such as updating your passwords or learning to spot phishing attempts, make a significant impact on your security. Consider reviewing your cyber hygiene in another 6–12 months to see how far you've progressed and identify any new areas for improvement. Your efforts not only protect you but also contribute significantly to the safety of our entire organization. Keep up the great work!