Employee Feedback

Cyber Hygiene Score

51.47%

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

Introduction

Your current cybersecurity hygiene stands in a moderate range, indicating some good practices but also considerable areas needing attention. Good cybersecurity habits are crucial not only for your protection but for the safety of the entire organization. By improving these habits, you contribute to a stronger, more secure digital environment for everyone.

What You're Doing Well

You’re already following essential practices that contribute significantly to cybersecurity. Keep up the great work in these areas:

- **Multi-Factor Authentication (MFA):** Using MFA adds an extra layer of security to your accounts beyond just a password.
- **Recognizing Phishing Attempts:** Being able to identify phishing emails helps protect both personal and company data from malicious attacks.
- **Reporting Suspicious Emails:** Informing the IT/security team about suspicious emails contributes to better security measures for everyone.
- **Avoiding Unauthorized Software:** Not using personal USB drives or unauthorized software prevents potential malware infections on work devices.
- **Remote Work Security:** Using a VPN or secured connection keeps sensitive work data safe from prying eyes.
- **Device Exclusivity:** Ensuring work devices are only used by you reduces the risk of accidental or deliberate data breaches.
- **Comfort in Reporting Issues:** Feeling comfortable to report mistakes or issues aids in quickly addressing and mitigating potential security threats.

Areas to Improve

Password & Access Management

- **Unique Passwords:** Using the same password for multiple accounts increases risk. Unique passwords minimize the impact of exposed credentials.

- **Secure Storage:** Store passwords safely using a password manager to protect them from unauthorized access.

- **Device Locking:** Always lock your devices when unattended to prevent unauthorized access to sensitive information.

Phishing Awareness & Email Security

- **Cybersecurity Training:** Participate in training to better recognize phishing tactics. Understanding these can prevent data breaches.

- **Verification Practices:** Always verify sender details before engaging with links or attachments to avoid malicious content.

Device & Data Security

- **Regular Updates:** Keep devices updated to protect against vulnerabilities. This includes operating systems, apps, and applying security patches.

- **Encrypted Communication:** For sensitive work discussions, use encrypted channels to protect information from eavesdropping.

Remote Work & Public Network Security

- **Avoid Public Wi-Fi:** Public networks are insecure and can be easily exploited. Use a secure connection when accessing company resources remotely.

Incident Reporting & Cybersecurity Culture

- **Incident Reporting Knowledge:** Ensure you know how to report cyber incidents promptly. Immediate reporting can minimize damage.

- **Participating in Exercises:** Join in simulated security exercises to practice handling incidents effectively.

Potential Risks and Risk Scenarios

- **Password Risks:** Reusing passwords means that a data breach on one site could expose your other accounts.

- **Phishing Vulnerability:** Without proper awareness, a phishing email could trick you into revealing sensitive information.

- **Outdated Software:** Running software without updates leaves your devices open to known attacks.

- **Insecure Remote Access:** Accessing company systems via unsecured connections can lead to data breaches.

Personal Cyber Hygiene Action Plan

Immediate (0–30 Days)

Quick wins and critical fixes:

- Use strong, unique passwords for each account.
- Enable multi-factor authentication wherever possible.
- Avoid clicking suspicious links or attachments.
- Update all software and operating systems.
- Restart your computer regularly to apply updates.

Short-Term (60–90 Days)

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

- Attend cybersecurity awareness training.
- Learn how to identify phishing and social engineering attempts.
- Review password manager options for better password handling.
- Ensure devices auto-lock after inactivity.

Medium-Term (3–6 Months)

Longer-term changes to build sustainable habits:

- Adopt a personal routine for monthly software updates.
- Explore and improve digital privacy settings across services.
- Develop safe remote work and travel security habits.

Conclusion

Keep improving your cybersecurity practices! Remember, small, consistent actions — like strengthening passwords or learning to spot phishing — can have a big impact on both your security and the organization’s. It’s a good idea to revisit your cyber hygiene and assess progress in the next 6–12 months. You're on the right path, and your efforts make a meaningful difference!