Employee Feedback

Cyber Hygiene Score

23.53%

Critical: Your cyber hygiene practices need urgent improvement.

Introduction

Hi there! Your current cybersecurity hygiene is considered weak based on your score. It's important to know that good habits are essential not only for protecting yourself but also for the security of your organization. Improving your cyber hygiene can help safeguard your personal information and help the company avoid potential cyber threats.

What You're Doing Well

Here are some areas where you're already doing a great job:

- **Device Updates:** Regularly updating your work device's operating system, applications, and security patches is crucial because it helps protect against newly discovered vulnerabilities and threats.
- **Error Reporting:** Being comfortable with reporting mistakes or security issues to IT is important for quickly addressing and mitigating any potential security problems.

Areas to Improve

Password & Access Management

- **Unique Passwords:** It's essential to use unique passwords for each of your accounts to prevent a single data breach from compromising all of them.
- **Password Storage:** Secure password storage, such as using a password manager, helps protect your credentials.
- **Multi-Factor Authentication (MFA):** Enabling MFA adds an extra layer of security to your accounts, making it significantly harder for unauthorized users to gain access.
- **Device Locking:** Locking your computer and devices when unattended prevents unauthorized access to your information.

Phishing Awareness & Email Security

- **Phishing Recognition:** Being able to recognize phishing emails ensures that you don't fall for scams that could lead to data breaches.
- **Training Participation:** Engaging in cybersecurity training helps you better understand and identify phishing attempts.
- **Email Verification:** Always verifying sender addresses before clicking links or attachments helps avoid malware and phishing attacks.
- **Reporting Suspicious Emails:** Notifying IT about suspicious emails provides a way to deal with threats before they escalate.

Device & Data Security

- **USB and Software Use:** Avoid using personal USB drives and unauthorized software on work devices to prevent the introduction of malware.
- **Encrypted Communication:** Using encrypted channels for sensitive discussions protects information from unauthorized interception.

Remote Work & Public Network Security

- **VPN Use:** A VPN ensures secure remote work connections by encrypting your internet traffic, especially on unsecured networks.
- **Public Wi-Fi Avoidance:** Avoiding public Wi-Fi for work tasks reduces the risk of data interception by malicious actors.
- **Device Usage:** Ensuring that work devices are only used by you helps maintain security controls.

Incident Reporting & Cybersecurity Culture

- **Incident Reporting:** Knowing how to report a cybersecurity incident is essential for prompt response to contain and mitigate threats.
- **Simulated Exercises:** Participating in cybersecurity exercises helps you practice and improve your response to potential threats.

Potential Risks and Risk Scenarios

Here are some potential risks based on the areas needing improvement:

- If you use weak or reused passwords, attackers could easily compromise your accounts.
- Without phishing awareness, you might fall for malicious emails and expose sensitive data.
- Running outdated software can leave your devices vulnerable to known exploits.

- Unsecured remote access can allow attackers to breach company systems.

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 striving to improve your cybersecurity practices. Remember that small actions, like updating passwords and learning to spot phishing attacks, can make a significant difference. Consider reviewing your cyber hygiene again in 6–12 months to track your progress.

By taking these steps, you'll be proactively protecting both yourself and your organization. Keep up the good work, and feel free to reach out if you have any questions or need support along the way!