Employee Feedback

Cyber Hygiene Score

23.53%

Critical: Your cyber hygiene practices need urgent improvement.

Introduction

Hello! Based on your current cybersecurity hygiene score, there's a bit of work to do. The score indicates that your practices are weak and need some urgent attention. The good news is that with a few changes, you can significantly improve your protection of both your personal data and our organization’s security. Good cybersecurity habits help prevent cyberattacks and keep everyone safer in today’s digital world.

What You're Doing Well

Let's start with the positives! Here are a couple of areas where you're already doing great:

- **Reporting Issues:** You feel comfortable reporting mistakes or security issues to the IT/security team. This is crucial because quick reporting can prevent small issues from becoming major problems.

Areas to Improve

Here are the areas where improving your habits could greatly benefit your security:

Password & Access Management

- **Unique Passwords:** It's important to use different passwords for each account to prevent a single breach from compromising all your accounts.
- **Secure Password Storage:** Make sure to store passwords securely, possibly using a password manager.
- **Multi-Factor Authentication (MFA):** Using MFA adds an extra layer of security and should be enabled whenever possible.
- **Device Locks:** Always lock your devices when leaving them unattended to protect against unauthorized access.

Phishing Awareness & Email Security

• **Phishing Recognition:** It's important to improve your ability to identify phishing emails to avoid falling for scams.

• **Training and Verification:** Participating in training can enhance your skills, and verifying sender addresses can prevent accidental clicks on harmful links.

• **Reporting Suspicious Emails:** Always report suspicious emails to IT/security promptly.

Device & Data Security

• **USB Drives and Software:** Avoid using personal USB drives or unauthorized software on work devices to prevent malware infections.

• **Encryption:** Use encrypted communication channels for sensitive discussions to protect data integrity.

Remote Work & Public Network Security

• **Secure Connections:** Always use a VPN or a secured connection when working remotely, and avoid public Wi-Fi for work tasks.

• **Device Sharing:** Ensure that work devices are not used by family or friends to maintain the integrity and security of the device.

Incident Reporting & Cybersecurity Culture

• **Incident Reporting:** Ensure you know how to report a cybersecurity incident promptly.

• **Security Drills:** Participating in cybersecurity exercises helps you respond effectively to real threats.

Potential Risks and Risk Scenarios

Here are some risks associated with current weak areas:

• **Password Risks:** If you reuse passwords, a breach on one site could expose all your accounts.

• **Phishing Attacks:** Without increased awareness, you might click on malicious emails, risking data exposure.

• **Outdated Software:** Running outdated software could make your devices vulnerable to exploits.

• **Remote Access Risks:** Unsecured remote access could allow attackers to penetrate company systems.

Personal Cyber Hygiene Action Plan

Immediate (0–30 Days)

Let's tackle some quick wins:

- Start using strong, unique passwords for each account right away.
- Enable multi-factor authentication on all accounts that offer it.
- Be cautious with email links and attachments – avoid anything suspicious.
- Update all your software and operating systems immediately.
- Regularly restart your computer to ensure updates are applied.

Short-Term (60–90 Days)

Here’s what to focus on in the next few months:

- Attend a cybersecurity awareness training session.
- Learn to spot phishing and social engineering tactics.
- Explore using a password manager to keep your passwords secure.
- Set your devices to auto-lock after a short period of inactivity.

Medium-Term (3–6 Months)

These longer-term habits will provide sustained benefits:

- Set a personal routine for monthly software updates.
- Review and improve digital privacy settings on all services you use.
- Establish and practice secure habits when working remotely or traveling.

Conclusion

Keep moving forward! Remember, small actions like updating passwords more frequently or learning to identify phishing scams can have a huge impact on your and your organization's security. Consider reviewing your cyber hygiene in 6 to 12 months to see how far you've come. Your diligence in improving these habits is invaluable, and I'm here to support you on this journey every step of the way.