Employee Feedback

Cyber Hygiene Score

73.53%

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

Introduction

Your current cybersecurity hygiene is moderately strong, reflecting a good foundation in digital safety practices. Strong cybersecurity habits are crucial not only for protecting yourself but also for safeguarding the organization's sensitive information. By continuously improving these practices, you'll contribute significantly to a safer digital environment for everyone.

What You're Doing Well

You're already making great strides in your cybersecurity practices. Here are some areas where you're excelling:

- **Multi-Factor Authentication (MFA):** Using MFA adds an extra layer of security, making it harder for unauthorized users to access your accounts.
- **Locking Devices:** Securing your devices when unattended helps prevent unauthorized access to sensitive data.
- **Phishing Recognition:** Being aware of phishing emails reduces the risk of falling for scams that aim to steal your personal and work information.
- **Verifying Sender Addresses:** Checking sender details before interacting with emails helps in identifying fraudulent communications.
- **Regular Updates:** Keeping your software up-to-date ensures you have the latest security protections and performance enhancements.

Areas to Improve

Let's take a closer look at some areas that could use a bit more attention:

Password & Access Management

- **Unique Passwords:** Using unique passwords for different accounts is essential. If one account is compromised, unique passwords prevent exposure to others.

• **Secure Password Storage:** Consider using a password manager to securely store and manage your passwords, reducing the risk of unauthorized access.

Phishing Awareness & Email Security

• **Training on Phishing Attacks:** Participating in training will enhance your ability to identify and respond to phishing attempts effectively.

• **Reporting Suspicious Emails:** It's important to report suspicious emails to IT/security immediately, helping to mitigate potential threats.

Incident Reporting & Cybersecurity Culture

• **Reporting Cybersecurity Incidents:** Knowing how to properly report cybersecurity incidents ensures that issues are addressed quickly and effectively.

• **Participating in Simulated Exercises:** Engaging in exercises like phishing tests can enhance your practical knowledge and readiness.

Potential Risks and Risk Scenarios

Some potential risks based on these areas include:

• **Password Risks:** Reusing passwords could lead to multiple accounts being compromised if a single site is breached.

• **Phishing Risks:** A lack of phishing awareness might lead to accidentally sharing sensitive information with malicious actors.

Personal Cyber Hygiene Action Plan

Immediate (0–30 Days)

Quick wins and critical fixes:

• Develop strong, unique passwords for each account.

• Enable multi-factor authentication wherever it's available.

• Be cautious and avoid opening suspicious links or attachments in emails.

• Update all your devices and software to their latest versions.

• Regularly restart your computer to ensure updates are applied.

Short-Term (60–90 Days)

Mid-term improvements:

- Attend cybersecurity awareness training sessions.
- Learn techniques to identify phishing and social engineering attempts effectively.
- Consider using a password manager for improved password security.
- Configure your devices to auto-lock after a period of inactivity.

Medium-Term (3–6 Months)

Longer-term habit formations:

- Establish a routine to check for and apply software updates monthly.
- Review and adjust digital privacy settings across your various online services.
- Develop safe habits for remote work and travel, such as using VPNs.

Conclusion

Keep up the great work and continue striving to improve your cybersecurity practices. Remember, small actions like updating your passwords regularly or learning to identify phishing scams can significantly enhance your overall security. Consider evaluating your cyber hygiene again in 6–12 months to track your progress. Your dedication to cybersecurity plays an essential role in protecting both yourself and your organization.