# Employee Feedback

## Cyber Hygiene Score

55.88%

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

## Introduction

Your current cybersecurity hygiene, as indicated by your score of 55.88%, is moderate. While you have a foundation to build on, there are areas that require improvement to ensure you and our organization remain secure against cyber threats. Cultivating strong cybersecurity habits not only protects you but also helps safeguard the sensitive information and resources of the entire company.

## What You're Doing Well

Here are some areas where you're demonstrating solid cybersecurity practices:

- **Storing Passwords Securely:** Secure storage of passwords is crucial in preventing unauthorized access to your accounts.
- **Recognition of Phishing Emails:** This skill helps protect you from scams designed to steal personal or organizational data.
- **Comfort in Reporting Mistakes or Security Issues:** Reporting incidents ensures quick action can be taken to mitigate risks.

## Areas to Improve

### Password & Access Management

- **Unique Passwords:** Using the same password across accounts increases the risk of a data breach. Unique passwords for each account enhance security.
- **Locking Devices:** Always lock your devices when not in use, preventing unauthorized access to company data.

### Phishing Awareness & Email Security

- **Cybersecurity Training:** Regular training sessions help you stay on top of new phishing tactics.
- **Verifying Sender Addresses:** Always check sender details to avoid falling prey to impersonation attacks that can lead to data leaks.

### Device & Data Security

- **Regular Updates:** Ensure your operating systems, apps, and security patches are current to protect against known vulnerabilities.
- **Avoid Unauthorized Software:** Using unknown programs or personal USBs can introduce malware into your work environment.

### Remote Work & Public Network Security

- **Secure Connections:** Use VPNs for encrypted communication and avoid public Wi-Fi, which can be a hotspot for attackers.
- **Safe Remote Work Practices:** Developing secure habits when working remotely protects both personal and company data.

### Incident Reporting & Cybersecurity Culture

- **Reporting Incidents:** Familiarize yourself with the process to report cybersecurity events swiftly, minimizing potential damage.
- **Participating in Exercises:** Engaging in simulated tests enhances your skills in identifying and reacting to threats.

## Potential Risks and Risk Scenarios

- **Password Vulnerability:** If you reuse passwords, a single data breach can compromise multiple accounts.
- **Phishing Attacks:** Without sufficient awareness, you risk falling for emails that could lead to data breaches.
- **Outdated Software:** Leaving software unpatched invites exploitation by attackers aiming to exploit known vulnerabilities.
- **Unsecured Remote Access:** Without a secure connection, you may unintentionally allow access to company systems.

## Personal Cyber Hygiene Action Plan

### Immediate (0–30 Days)

- Create strong, unique passwords for all your accounts using a password manager.
- Enable multi-factor authentication wherever available.
- Be cautious of links or attachments from unverified sources.

- Update your operating system and all software immediately.
- Restart your computer regularly to ensure updates are applied.

### Short-Term (60–90 Days)

- Attend a cybersecurity awareness training session.
- Study common phishing and social engineering tactics.
- Research password manager tools for more secure password management.
- Set your devices to auto-lock after a short period of inactivity.

### Medium-Term (3–6 Months)

- Establish a routine for monthly updates on all software.
- Review and adjust privacy settings on services you use.
- Develop a secure practice routine for remote work, including how to handle data while traveling.

## Conclusion

---

Keep up the momentum in improving your cybersecurity practices. Remember, simple actions like updating passwords and learning to recognize phishing attempts have profound effects on security. Let's plan to review your progress in your cyber hygiene journey again in 6–12 months. Your efforts not only protect you but contribute significantly to the security of our whole team. Keep up the good work!