Employee Feedback

Thank you for participating in the cybersecurity self-assessment. It's crucial to recognize that a 0.00% score highlights significant vulnerabilities in your current practices, which may expose both personal and organizational data to potential threats. Key risks identified include the lack of unique passwords, unsecured password storage, and the absence of multi-factor authentication—all critical elements for protecting accounts against unauthorized access. Additionally, your current practices around device security, phishing recognition, and incident reporting need immediate attention to reduce risks of data breaches and phishing attacks. Another major concern is using unsecured connections for work tasks, such as public Wi-Fi, which can be exploited by malicious actors.

To improve your cyber hygiene, I highly recommend that you start with basic password management. Use unique, strong passwords for each account and consider a reputable password manager to store them securely. Implement multi-factor authentication wherever possible to add an extra layer of security. Prioritize attending cybersecurity training sessions to enhance your understanding of phishing threats and participate in exercises like simulated phishing tests to build practical skills. Update your devices regularly and ensure that unauthorized software or personal USB drives are not used on work devices. Always use a VPN for a secured connection when working remotely. As a fundamental practice, report any suspicious emails or security incidents to IT/security promptly. By addressing these critical areas, you can significantly strengthen your cybersecurity posture and contribute to a safer work environment.