Employee Feedback

■ Amazing Achievements!

You've nailed every aspect of cyber hygiene.. You're really showing that commitment to keeping both your personal and work information secure. Keep up the fantastic work! Here's what you're doing exceptionally well:

■ What You're Doing Well - Unique passwords for every account? ✔■ Stellar practice! - Storing passwords securely? ✔■ Gold standard! - Multi-factor authentication (MFA) in use? ✔■ Excellent! - Locking devices when unattended? ✔■ Perfect! - Phishing email awareness? ✔■ Absolutely on point! - Cybersecurity training participation? ✔■ Ahead of the game! - Verifying sender addresses? ✔■ Brilliant attention to detail! - Reporting suspicious emails? ✔■ True prevention star! - Regular updates on devices and apps? ✔■ Top-notch! - Avoiding personal USBs/software on work devices? ✔■ Great decision making! - Encrypted communication for sensitive talks? ✔■ Privacy champ! - Using a VPN for remote work? ✔■ Secure genius! - No public Wi-Fi for work? ✔■ Cyber-safety expert! - Keeping work devices personal? ✔■ Absolutely essential! - Incident reporting knowledge? ✔■ Confidence builder! - Adequate cybersecurity training at work? ✔■ Continuous improvement! - Participated in simulated exercises? ✔■ Proactive engagement! - Organization prioritization of cybersecurity? ✔■ Solid foundation! - Comfort in reporting mistakes or issues? ✔■ Cyber-safe culture!

■■ Areas to Improve

Amazing news — no areas need improvement at the moment. Your score is a perfect 100%!

■ Potential Risks

Even with your impeccable score, always stay vigilant for potential threats, including: - **Phishing risks:** Continue to be cautious as these attacks can be sophisticated. - **Password threats:** Maintain those unique, strong passwords to prevent unauthorized access. - **Software updates:** Although you update regularly, never let this slip to keep vulnerabilities at bay.

■■ Action Plan

■ Immediate - Remain diligent with email scrutiny—never let unusual links catch you off-guard. - Continue your excellent practice with long, unique passwords paired with MFA. - Maintain your habit of prompt software updates and continuous system reboots.

■ Next 2–3 Months - Why not deepen your knowledge with additional cybersecurity trainings? - Constantly refine your ability to spot social engineering tricks, such as impostor tech support calls.

Your current practices are stellar. Keep pushing forward with your proactive and outstanding approach to cybersecurity. You're setting a high standard and leading by example in your cyber-safe journey! ■■