Employee Feedback

Immediate (0–30 Days)

1. **Strengthen Password Practices:**

    • Begin using a password manager to create and store strong, unique passwords for every account. Password managers simplify the process and enhance security.

    • Ensure passwords include a mix of letters, numbers, and special characters for added security.

2. **Enable Multi-Factor Authentication (MFA):**

    • Activate MFA on important accounts, especially email and financial services. This adds an extra layer of security by requiring more than just a password to access accounts.

3. **Keep Devices Secure and Updated:**

    • Regularly update the operating systems, apps, and security patches on your devices. This helps protect against vulnerabilities.

    • Develop the habit of locking your computer and devices when you leave them unattended.

4. **Basic Awareness on Phishing:**

    • Be cautious of emails or messages that urge you to click on links or open attachments, especially if they're unexpected. Verify the sender's address carefully.

Short-Term (60–90 Days)

1. **Engage in Cybersecurity Training:**

    • Enroll in cybersecurity workshops or courses offered by your organization. This will enhance your understanding of common threats and how to handle them.

    • Focus on identifying phishing emails and other social engineering tactics.

2. **Increase Reporting and Communication:**

    • Familiarize yourself with the process of reporting suspicious emails and cybersecurity incidents to your IT/security team. Remember, prompt reporting helps prevent potential breaches.

    • Build a comfort level in discussing any cybersecurity concerns or mistakes with IT. Transparency can lead to quicker resolutions and learning opportunities.

3. **Secure Remote Work Practices:**

- Use a VPN whenever working remotely to secure your internet connection.
- Avoid using public Wi-Fi for work-related tasks. If necessary, use a hotspot or VPN to ensure your data is safe.

4. **Limit Device Access:**

- Ensure only you use your work devices, minimizing the risk of accidental exposure to threats from others.

Remember, improving your digital hygiene is a step-by-step journey. Each small action contributes significantly to enhancing your cybersecurity posture. Stay motivated, stay secure, and don't hesitate to ask for help when needed. You've got this!