Employee Feedback

Feedback

You’re Off to a Great Start!

First off, congratulations on your excellent practices! You are doing extremely well in several critical areas, which are essential for maintaining robust cybersecurity hygiene. Keep up the great work with using unique passwords, storing them securely, enabling multi-factor authentication (MFA), and verifying sender addresses. You clearly understand the basics and importance of securing your digital environment, which is crucial in today's cyber landscape.

Areas for Improvement

Fortunately, with a little focus in the right areas, you can further enhance your cybersecurity measures. Here are some structured, actionable steps to guide you on this path:

1. Secure Communications:

- **Action:** Begin using encrypted communication channels for sensitive work discussions. Whether it’s email, chat, or calls, ensuring these are encrypted can safeguard your data from eavesdropping and interception.
- **Tip:** Explore options such as Signal or encrypted email services for secure communications.

2. Remote Work Security:

- **Action:** Implement the use of a VPN or secure connections when working remotely, and avoid public Wi-Fi for any work tasks to prevent unauthorized access to your data.
- **Tip:** Set up a VPN on your devices and make it a habit to connect through the VPN anytime you're working remotely.

3. Device and Personal Use:

- **Action:** Ensure that family members or friends do not use your work devices to prevent accidental modifications or security breaches.
- **Tip:** Communicate with family members about the importance of digital security and set boundaries around device usage.

4. Incident Reporting and Training:

- **Action:** Familiarize yourself with the procedure for reporting cybersecurity incidents within your organization if you aren't already completely sure.

• **Tip:** Review your company’s reporting policies and identify the points of contact for cybersecurity issues.

5. Organizational Support and Involvement:

• **Action:** Advocate for more cybersecurity training within your organization, including participation in simulated exercises like phishing tests.

• **Tip:** Approach your IT/security team to express interest in more frequent training and simulations to keep skills sharp.

Potential Risks Recap:

• There's always a potential risk of falling for phishing emails. Strengthen your awareness with regular training.

• With your excellent practices, weak password habits are a minimal risk, but keep maintaining strong passwords and MFA.

• Keep software and devices up-to-date to eliminate vulnerabilities from outdated software.

Friendly Encouragement:

You're on the right track and have already conquered some of the trickiest aspects of cybersecurity. By focusing a bit more on the areas highlighted, particularly in secure communications and remote work practices, you can elevate your cybersecurity stance significantly. Remember, the goal is not just to protect yourself, but also to strengthen your organization’s overall security. Keep up the great work, stay informed, practice regularly, and encourage your organization to support further training and security initiatives. You’ve got this!