Employee Feedback

Feedback: Improving Your Cybersecurity Practices

Hello! It's great that you're taking steps toward enhancing your cybersecurity habits. A few key practices are already part of your routine, and I'm here to help you build on those strengths while addressing areas that need improvement. Let's dive into what you're doing well and how you can enhance your digital hygiene further.

What You're Doing Well

You've made excellent progress in a few critical areas:

- Receiving training on phishing attacks shows your commitment to staying informed.
- Verifying sender addresses and reporting suspicious emails demonstrates a proactive approach to email security.
- Keeping your devices updated regularly is a solid protective measure.
- Using authorized devices and encrypted communication channels is crucial for maintaining data integrity.

Areas to Improve & Action Plan

Immediate (0–30 Days)

1. **Password Management**
   - Use a password manager to generate and store unique passwords for every account. This will simplify access management and heighten security.
   - Enable Multi-Factor Authentication (MFA) wherever possible to add an extra layer of security.
2. **Device Security**
   - Make it a habit to lock your devices whenever you step away, even for a moment.
   - Familiarize yourself with the steps to report a cybersecurity incident within your organization, ensuring a quick response if needed.
3. **Phishing Awareness**
   - Review common signs of phishing emails, such as inconsistent email addresses, spelling errors, or urgent requests for sensitive information.

Short-Term (60–90 Days)

1. **Training & Exercises**

    • Enroll in and actively participate in cybersecurity training sessions provided by your organization.

    • Engage in simulated phishing exercises to improve your detection skills and gain confidence in identifying threats.

    • Encourage feedback and ensure regular communication with IT/security to understand new potential threats.

2. **Remote Work Protocols**

    • Avoid using public Wi-Fi for work tasks when possible, and if necessary, always use a VPN to protect your connection.

    • Keep your work devices exclusive to you. Ensure family and friends understand the importance of this practice.

3. **Organizational Involvement**

    • Reflect on your perception of the organization's cybersecurity prioritization and training sufficiency. Share this feedback with your team and IT department to foster a culture of improvement and awareness.

    • Reassure yourself that reporting any mistake or security issue is a positive action, contributing to a safer environment.

Remember, cybersecurity is a team effort, and every action you take strengthens the overall defense of your organization. Your progress is acknowledged and valued, and with targeted improvements, you'll be making significant strides. Keep up the excellent work, and don't hesitate to reach out for support along the way!

Stay safe and secure!