Employee Feedback

Feedback and Action Plan

Hello! First off, congratulations on your current cybersecurity practices — you're on the right track, and it's clear that you're mindful of your digital security. Let's build on this strong foundation and tackle those areas where you can enhance your digital hygiene even further.

What You're Doing Well

Your commitment to cybersecurity is evident in several key areas:

- **Multi-Factor Authentication**: By using MFA, you add an extra layer of defense.
- **Device Security**: Locking your devices when not in use protects sensitive information.
- **Phishing Awareness**: Recognizing phishing emails and verifying sender addresses are crucial skills.
- **Regular Updates**: Keeping your devices up to date with the latest patches safeguards against vulnerabilities.
- **Safe Communication**: Using encrypted channels and VPNs ensures privacy in your work discussions.
- **Work Device Usage**: By avoiding personal USB drives and restricting family access, you maintain the integrity of your work systems.

Areas to Improve

Here's where small changes can make big differences:

1. **Unique Passwords**: Using the same password across multiple accounts can compromise your security. Begin by using a password manager to help generate and store unique passwords for each of your accounts.

2. **Password Storage**: Make sure you're storing passwords securely by avoiding writing them down or saving them in unsecured digital formats.

3. **Cybersecurity Training**: Engaging in regular training keeps you alert to new phishing tactics and other threats.

4. **Incident Reporting**: Familiarize yourself with how to report suspicious emails and incidents to IT/security. This not only protects you but also helps safeguard your entire organization.

5. **Simulated Exercises**: Participate in phishing simulations and other cybersecurity exercises to enhance your response during real incidents.

Potential Risks

- **Phishing Emails**: Increased awareness and training will reduce the risk of falling for phishing schemes.
- **Weak Password Habits**: Addressing this can greatly enhance your personal and organizational security posture.
- **Outdated Software Vulnerabilities**: Although you are updating your systems, consistently ensuring this will prevent new vulnerabilities.

Action Plan

Immediate (0–30 Days)

- **Strengthen Passwords**: Begin using a password manager to create and store unique, strong passwords for all accounts.
- **Security Awareness**: Stay vigilant and avoid clicking on any suspicious links. If in doubt, always verify the source.
- **Device Maintenance**: Ensure your devices are updated with the latest patches and remember to restart them regularly to apply these updates.

Short-Term (60–90 Days)

- **Engage in Training**: Participate in cybersecurity training sessions offered by your organization. This will keep you updated on potential threats and how to tackle them.
- **Social Engineering Defense**: Spend time learning how to identify and block social engineering attempts, which are increasingly sophisticated.

Your awareness and willingness to improve are commendable. By focusing on these actionable steps, you're not just protecting yourself but also contributing to a safer digital environment for everyone around you. Keep up the great work, and remember, cybersecurity is a shared responsibility — together, we make our digital spaces secure!