Name: Irawansyah

NIM : 0320230124

Class : 2A

MEMO

To: All Employees
From: IT Department
Date: November 29, 2024
Subject: Enhancing Cybersecurity Awareness and Protection

Opening Statement

The safety and security of our digital infrastructure are critical to the success of our organization. Cybersecurity threats continue to rise, and it is essential for all employees to understand their role in protecting sensitive information and maintaining system integrity.

Context

Recent reports have highlighted an increase in phishing attacks, malware infiltration, and data breaches targeting businesses like ours. These threats can compromise not only our internal systems but also the personal data of our clients and partners. To mitigate these risks, a collective effort from every team member is necessary.

Call to Action and Task Statement

To enhance our cybersecurity posture, we are implementing several mandatory practices that all employees must follow:

1. **Password Security:**
    - Create strong, unique passwords for all accounts.
    - Update passwords every 90 days.
    - Avoid using personal information in passwords.
2. **Email Vigilance:**
    - Be cautious of unsolicited emails and verify the sender before clicking links or downloading attachments.
    - Report any suspicious emails to the IT Department immediately.

   -

3. **Software Updates:**
   - Regularly update your operating system and applications to the latest versions.
   - Enable automatic updates wherever possible.
4. **Use of VPN:**
   - Always use a company-approved Virtual Private Network (VPN) when working remotely to secure your connection.
5. **Data Backup:**
   - Backup important files regularly and store them in secure locations.

Discussion

To further support these efforts, the IT Department will host a **Cybersecurity Awareness Training** on **December 5, 2024**, at 10:00 AM in the main conference room. Attendance is mandatory for all employees. This session will cover:

- Identifying and avoiding phishing scams.
- Securing personal and professional devices.
- Proper data handling practices.

We encourage everyone to actively participate in the discussion and ask questions to clarify any doubts regarding cybersecurity practices.

Closing

Your cooperation is vital in protecting our organization from cyber threats. By adhering to these guidelines, you help safeguard our digital assets and maintain the trust of our clients and partners. Should you have any questions or require further assistance, please contact the IT Department.

Thank you for your attention and commitment to enhancing our cybersecurity.

IT Department
[CyberShield Inc]