PROTECT MY RESTAURANTS

Phishing Prevention Best Practices

1. **Recognize Phishing Emails**
    - Be suspicious of emails that request personal information or ask you to click on a link or open an attachment.
    - Look for poor grammar, spelling mistakes, and unfamiliar email addresses.
    - Check the sender's email address carefully for subtle misspellings or unusual domains.
2. **Verify Links Before Clicking**
    - Hover over links to see the actual URL before clicking. Ensure it matches the expected destination.
    - Avoid clicking on links in emails from unknown or untrusted sources.
3. **Be Cautious with Attachments**
    - Do not open attachments from unknown senders, as they may contain malware or viruses.
    - Even if an email appears to be from someone you know, be cautious if the message is unexpected or out of character.
4. **Use Anti-Phishing Software**
    - Install and maintain up-to-date anti-phishing and antivirus software to help detect and block phishing attempts.
    - Use browser settings and extensions that provide phishing protection.
5. **Educate Employees and Staff**
    - Regularly train employees to recognize phishing attempts and respond appropriately.
    - Encourage reporting of suspicious emails or messages to the IT or security team.
6. **Verify Requests for Sensitive Information**
    - Always verify requests for sensitive information by contacting the person or organization directly using known contact details.
    - Never provide personal or financial information in response to unsolicited requests.