PROTECT MY RESTAURANTS

Password Security Best Practices

1. Use Strong and Unique Passwords
   - Create passwords that are at least 12 characters long, using a mix of uppercase and lowercase letters, numbers, and special characters.
   - Avoid using easily guessable information like names, birthdays, or common words.
   - Use a unique password for each account to prevent a breach on one site from affecting others.
2. Use a Password Manager
   - Password managers can securely store and generate strong passwords for you.
   - They help you manage multiple passwords without the need to remember each one.
3. Enable Two-Factor Authentication (2FA)
   - Whenever possible, enable 2FA for an added layer of security.
   - This typically involves receiving a code on your phone or email in addition to entering your password.
4. Regularly Update Passwords
   - Change your passwords regularly, especially if you suspect they may have been compromised.
   - Update passwords immediately if there is any indication of a security breach.
5. Avoid Reusing Passwords
   - Using the same password across multiple sites increases the risk of multiple accounts being compromised.
   - Always create new, unique passwords for each site and account.
6. Be Cautious of Phishing Scams
   - Phishing attacks often attempt to steal passwords. Be wary of unsolicited emails or messages asking for your login information.
   - Verify the legitimacy of emails and websites before entering your password.