Password Security and Safe Applications

BANK OF THE WEST
BNP PARIBAS

You can have up to 85 passwords for all of your accounts when you include social media, streaming services, bank accounts, and other applications. It is highly advised users create unique passwords for each of your various accounts. Companies reported over 5,000 data breaches in 2019 exposing sensitive information with some data containing login credentials.

How can you keep track of all these passwords and what makes a secure password?

Secure Password

- Unique
  - Use a different password for every account
- At least 8 characters long and memorable
  - Create a passphrase that is easy to remember but hard to guess
  - Make a password from the first letter of each word in your passphrase
  - Substitute special characters for letters and include numbers
  - Example: my first job was at Bank of the West as a teller = M1jw@BotWaAt
- Avoid using personal information and common words
- Check the security of your password at How Secure is my Password

Use a Password Manager

- Password managers save passwords in one location
  - Can recommend secure passwords for your accounts
  - Can be synced across multiple devices for ease of use
- Take time to research reviews and reputations of password managers to find a best fit

Find Out if Your Password has been Exposed

- Check if your password has been disclosed in a breach at Have I Been Pwned
- Check for compromises and password strength of your stored Google account passwords at Google Password Checkup

Third Party Applications

- Third party software applications may contain features allowing for device compromise and personal information leaks
- Only download applications from official sources such as Apple AppStore and Google Play
- Check application privacy settings periodically
- Look at application reviews before you download them; scammers will upload apps that mimic legitimate apps
- Download mobile antivirus software; applications are available for Android and iPhone
- Apps should be given as few permissions as possible
  - Set privacy settings to ensure apps are not using or sharing location data
  - Avoid using apps related to location if possible. If used, location privacy/permission settings for such apps should be set to either **not** allow location data usage or, at most, allow location data usage only while using the app