Protecting Your Personal Information

BANK OF THE WEST
BNP PARIBAS

Your personal information requires constant vigilance and it can be easy to let your guard down. Fraudsters and criminals are constantly on the lookout for data useful for their gain. Some personal information should be protected higher than others. Your name, address, and phone number can be found fairly easily but this information can be used against you in a targeted attack. Your date and place of birth as well as your mother's maiden name should be protected more carefully. Fraudsters skilled in social engineering may attempt to gather this information from you. You may see posts on social media asking innocuous questions about individuals, this may be an attempt to gather information from you in order to answer questions you have setup for password resets on accounts. The most sensitive personal information to protect includes your bank account numbers, social security, PIN, credit card numbers, and passwords. The following are tips everyone can use to their advantage to keep their personal data out of the wrong person's hands.

Create Strong Passwords

Using a strong and separate password for all of your online accounts is one of the best ways to protect your accounts. A recommendation is to use a password management tool such as LastPass, 1Password, or Dashlane, which will store your passwords and help you generate a new password when a new account is opened or you decide to change an account.

Multi-Factor Authentication

To increase your account privacy even further, use multi-factor authentication, this adds a second layer of protection. It is recommended to use an application like Google Authenticator, if available, or enable SMS authentication if it is the only option.

Set Privacy Settings

You should periodically check their privacy settings on every social media account. These settings control the type of information shared publicly and with friends. The safe option is to only allow your friends to see your posts, comments, and profile information. Privacy settings change over time and do not be surprised when you check settings you may be sharing more information than you were aware. Do not share information with websites or apps connected to your social media accounts. This information can be collected and sold to advertisers, or worse, become part of a data breach and found in the hands of criminals.

Do Not Fall for Phishing

Your personal accounts are susceptible to phishing attempts just like your work accounts. One of the leading attack methods for criminals is phishing. By casting out a wide net, they are hoping one or two people will click a link or respond in order to install malicious software or capture your personal information. Phishing is not limited to email, suspicious text messages are also being sent to provide control of your mobile device to malicious actors. Use caution when you receive a message from someone you do not recognize with a request to click a link or take urgent actions. Look for spelling errors in emails, salutations not including your name, and email addresses or website addresses in the message not lining up with what the email is talking about or the company allegedly sending you the email.