CONSUMER TIPS

Tips when using mobile devices for financial services

Many consumers use mobile devices for financial services to save time when accessing accounts, help track spending, and manage money. Using mobile devices is a lot like using a computer, and you should use similar best practices for security—especially since your mobile device can get lost or stolen.

Here are some tips for using your mobile device more safely and securely to help you achieve your financial goals.

- Set up alerts and check your account balances: You can set up alerts by text message, email, or even app notifications. Alerts can tell you when your checking account balance is low, when your credit card balance exceeds a limit you set, and even when a charge over a specified amount is placed on your credit card.
- Protect your personal information: Don't share your PIN or password with anyone, and don't save them on your mobile device. Think twice about accessing your accounts on a phone or device that you share with another person.
- Use passwords: Password protecting your mobile device can help prevent access to your information in the device. Don't use easily identifiable passwords like your birthday and never save passwords on your phone.
- Report loss or theft to all your financial institutions or financial services providers as soon as it occurs. If you lose your mobile device, you may be focused on notifying the mobile provider -- but don't forget to report loss or theft to your financial providers if your device can provide access to your accounts through apps.
- Use secure websites or apps: This sounds obvious, but don't login to your accounts through links that are sent to you by an email address or on a website or app that you don't recognize. When using free or public wi-fi, try to use a private network and go to a secure site that begins with HTTPS.
- Remove sensitive information from your old phone or device: If you get a new phone or mobile device, be sure to delete your data and information from the old phone. You may have left names of banks or credit unions, passwords, or other clues that could help identify your personal information.