FDIC

October 28, 2019

FEDERAL DEPOSIT INSURANCE CORPORATION

consumer news

Banking at the Speed of Technology

Follow these tips to help ensure your money stays secure

Millions of people today use mobile devices to manage their finances, and the number of users continues to grow. Why? Mobile banking technology and services provide so much convenience. You can access your account from just about anywhere using a smartphone or mobile computer device today. As demand grows, the banking industry strives to improve online services while keeping customers' funds safe.

Money Transfer Services:
Person-to-person payment services and mobile payment apps have become part of everyday life for many people. Payment services and apps let you send money to people without having to write a check, swipe a card, or hand them cash. These services are becoming increasingly popular for things like dividing the cost of rent with a roommate or tracking costs and splitting the bills when traveling. With the development of new payment methods, there are also new risks, so keep the following in mind when using these services and apps:

Have your friend send you a request for payment first. If you're sending money to someone for the first time, ask that they send a "request" from their app, if that service is available. This helps ensure that you're sending funds to the right person for the right amount. If the payment app does not have a request for payment function, consider sending a small, test payment to the recipient to confirm it is the right person before sending larger amounts.

Double-check before you press that send button. A simple mistype can send money to the wrong person or the wrong amount. Always double-check the amount you entered and the person you selected to pay. Most payment apps require a username, phone number, or email address to identify payment recipients. Ask the recipient to be sure he or she is registered in the app with the information you intend to use to send them money. You can sometimes "stop payment" with written checks, dispute a credit card charge, or cancel a bill payment, but mobile payment services generally don't have a recall or retrieval feature. For these reasons, it's important to be certain you want to make a payment via transfer, then verify how much and to whom before pressing send.

Know when to expect to receive transferred money or when it should leave your account. You may have to wait to spend money you receive in a transfer. Even if the money appears to be in your balance instantly, you may not be able to spend the money as quickly as it shows up, so be sure to read the disclosures to find out how much time they have to complete the transaction. When you send money via mobile apps, most payments

get deducted from your balance immediately.

Depositing checks using Remote Deposit Capture:
Many banks allow customers to use Remote Deposit Capture (RDC), which allows customers to take a picture of a check with their mobile device and deposit that check electronically without ever visiting a branch or using an ATM. This service is becoming popular, especially among customers who don't live or work close to a bank branch. If you use RDC, carefully track the checks you deposit. For example, you might write the date you deposited the item on the front of the paper check and hold onto it until the check has cleared and the money is in your account. Once the deposit is verified, you can destroy the check, preferably using a high-quality paper shredder. Ask your bank more about how this service works.

Additional tips for mobile banking:
Set account alerts. Most mobile banking systems allow you to sign up for alerts on your mobile device or email to notify you if your account balance drops below a set dollar amount and thereby help you avoid overdrawing from your account. You may also be able to receive text alerts if your bank observes suspicious or potentially fraudulent transactions involving your account. Some systems even let you set spending limit alerts to help keep track of your spending.

Research apps before downloading. Just because the name of an app resembles the name of your bank or another company you're familiar with, that doesn't mean it is their official app. Fraudulent apps are created all the time, so verify that you have the correct one before adding any personal information to your new app.

Be on guard against unsolicited email or text messages appearing to link to a financial institution's website. Those could be "phishing" messages, which often contain an urgent request (such as a warning that you need to verify bank account or other personal information). Sometimes it is disguised as an amazing offer, designed to lure you to a fake website where fraudsters hope to steal your information and ultimately your funds. *Learn more about phishing scams by visiting:* https://www.fdic.gov/consumers/consumer/news/cnsum17/scams.html.

Be proactive in securing your mobile device. Never leave your mobile device unattended and make sure you enable the auto-lock feature to secure your mobile device when it is left untouched for a period of time. Be sure to create a strong password or PIN on your mobile device and don't make it obvious (like your birthday or social security number). You should periodically change your pin or password, which also helps keep it secure. Most importantly, don't give that password or PIN to anyone, or write it down where others can find it, especially with the device. You may also want to consider using a mobile device with a biometric authentication method, which verifies your identity by scanning your physical characteristics, such as your fingerprint or face.

Be careful where and how you conduct transactions. Don't use unsecured Wi-Fi networks to conduct your private business. Fraud artists might be able to access the information you are transmitting or viewing. Also, don't send account numbers or other sensitive information through regular email or text messages, because they are also vulnerable to hackers.

If your mobile banking services are not functioning properly, it might be due to technical difficulties. Be sure to contact the service provider as soon as possible to resolve this issue.

Take additional precautions if your device is lost or stolen. Check with your wireless provider in advance to find out about features that enable you to remotely erase content or turn off access to your device or account. Contact your financial services providers to let them know about the loss or theft of your device. Notifying your bank quickly will help prevent or resolve problems should any unauthorized transactions occur as a result.

For more helpful tips on banking and technology, visit:
Federal Deposit Insurance Corporation
https://www.fdic.gov/consumers/consumer/news/cnwin16/
https://www.fdic.gov/bank/analytical/fintech/
Federal Trade Commission
https://www.consumer.ftc.gov/blog/2018/02/tips-using-peer-peer-payment-systems-and-apps

For more help or information, go to **www.fdic.gov** or call the FDIC toll-free at **1-877-ASK-FDIC (1-877-275-3342)**. Please send your story ideas or c omments to Consumer Affairs at **consumeraffairsmailbox@fdic.gov**

FDIC