Mobile Payment Apps: How to Avoid a Scam When You Use One

Mobile payment apps can be a convenient way to send and receive money with your smartphone. These apps have become very popular — and scammers may try to use them to steal your money. Find out how mobile payment apps work and how to avoid sending money to a scammer.

How Mobile Payment Apps Work

You may have heard of mobile payment apps like Venmo, Cash App, or Zelle that let you send and receive money through your smartphone. If you haven't used one before, here's how they work.

To use a mobile payment app, you'll have to create an account. You may have to link your mobile payment account to your bank account or credit card.

> ***Security Tip:*** *Check if you can turn on additional security features on your account. You may want to use multi-factor authentication, create a PIN, or use fingerprint recognition.*

Once you set up the account, you may be able to use the app to make payments at some stores.

You can also send money to people you know — just make sure you're sending money to the right person. Double-check their email address, phone number or username.

And people can use the app to pay you. When someone sends you a payment, the money doesn't go to your bank account. Instead, it will appear in your app's account balance. You can then decide what to do with the money. You can

- leave the money in your mobile payment account
- send that money to someone through the app
- transfer the money to your bank account

How to Avoid Sending Money to a Scammer

For years, scammers have been making up all kinds of stories to trick people into sending them money. They may lie to you and say

- you won a prize or a sweepstakes and need to pay some fees to collect it
- a loved one is in trouble and they need you to send money
- you owe taxes to the IRS
- they're from tech support and need money to fix a problem with your computer
- they're someone who is romantically interested in you and needs some money

Scammers want you to pay in a way that's quick and makes it hard for you to get your money back. That's why they'll tell you to wire money or pay them with reload cards or gift cards.

Scammers may also tell you to send money through a mobile payment app. If you get an **unexpected** email or text message that asks you to send money, don't click on any links. Log in to the app to see if you have any requests for money. If you don't, the email or text is probably a phishing scam.

What to Do If You Sent Money to a Scammer

If you sent money to a scammer, report the scam to the mobile payment app and ask them to reverse the transaction right away.

Then, report it to the Federal Trade Commission. When you report a scam, the FTC can use the information to build cases against scammers.