Mobile Payment Scams to Avoid

How payment apps make it easier for scammers to get your money

Apps that allow you to conduct transactions directly from your mobile phone have been quickly growing in popularity. Unfortunately, scammers now try to take advantage of this convenience by tricking you into inadvertently sending them money. The following information may help you avoid this.

How mobile payment apps work

To understand how mobile payment scams work, it's useful to understand how mobile payment apps work. These apps, such as Zelle, Venmo, and Cash App, usually require you to create an account that you must then link to your credit card or an account at your financial institution.

Once this is set up, you can then use the apps to make payments at stores. Also, and this is the part that scammers care about in particular, you can use mobile payment apps to send money to people you know. Usually, all you need is their username, phone number, or email address.

People can also do the same to send you money, and if they do, you can do a few things with it. You can transfer it directly to your financial account, send it to someone else via the app, or simply leave it be until you want to use it. The convenience that mobile payment apps bring to sending money is what makes them so useful for scammers. The fewer steps you have to take to send them money, the less you're likely to think twice about the whole thing.

How scammers attempt to get your money

Scammers have always made up stories to try to convince their targets that they should send them money. They'll call your phone number and say you owe taxes to the IRS, make a window pop up in your internet browser that says tech support needs to fix something on your computer, pose as a family member who needs emergency money, announce you've won a prize but that collecting it comes with a fee, or even try to lure you into a romance scam.

These scams have existed long before mobile payment apps and will continue to exist in the future. But mobile payment apps have made it much easier for scammers to get the money. After all, if an app makes paying someone you know more convenient, it can make paying an illegitimate party easier too.

Fraud.org's John Breyault urges caution when you use P2P financial platforms. "All you need to get the money is a cellphone number or email address. That's why it's so important for people to be really careful when they're using these apps."

Sometimes, it can be tough to recognize scams, and scammers are always getting creative with their stories. When using mobile payment apps, however, the general rule is simple: if someone is asking for money and you don't know them personally, do not send them money. And if you do know them personally, get in touch with them directly — preferably in a way that leaves no doubt as to their true identity, such as in-person or via video call — to find out if the request truly came from them.

Lack of fraud protection

Unlike the money you have stored in an account with your financial institution, the money you spend via a mobile payment app is not well protected. Justin Higgs, director of corporate affairs at Venmo, says you shouldn't use the company's app to shop online, but only to give money to someone you know personally. "Venmo is designed for payments between friends and people who know and trust each other," he told NBC News, adding that the app's user agreement states it shouldn't be used to accept or send payment to other users for goods and services.

“People need to understand that a third-party company manages these apps,” said Amy Nofziger, director of the AARP Fraud Watch Network. This means you typically have fewer protections than traditional payment methods like debit and credit cards or checks.
In other words, once you send the money, it’s probably gone forever. The U.S. Federal Trade Commission says that if you sent money to a scammer, you should report the scam to both it and the mobile payment app, and then ask the app to reverse the transaction right away. But odds are the request will be declined, making it all the more important that you don’t fall for the scam in the first place.