

5 Payment App Scams & How to Avoid Them



Pelican State
credit union®

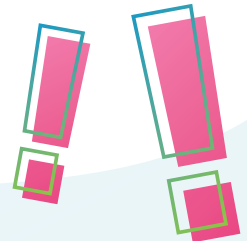
Your Financial Family for Life™



From mowing grass and babysitting to dining out with friends, you may find that your child would benefit from having a payment app for their convenience and yours.

With fraudsters and thieves stealing money using these apps, it can be nerve-racking for a parent. To protect your child from scammers, help them become familiar with some common payment app scams and how they can avoid them!

5 Scams to Watch Out For



1 Faux Customer Support

This type of scam can happen in a couple different ways. If you encounter an issue using the app and search for the app's customer support service number online, you may find a number on Google that isn't on the official app's website. This number directs you to a person imitating a customer support representative who will ask questions allowing them to login to your account.

Another way this happens is when the scammer tries signing into your account and encounters the app's multi-factor authentication process. This process will send a code to your phone number. The scammer will call you pretending to be the app's customer support asking for the code.

2 "You Won Money" Lies

You'll receive a link saying you won money from a number pretending to be the app. When you click the link, it will ask for your login information.

This also happens on social media with accounts pretending to be the apps. They will message users saying they won giveaways and to transfer a couple dollars to the app's fake account or send their login credentials for a chance to win.

3 Cryptocurrency Claim Scams

Users posing as fake celebrities and influencers will reply to comments, videos, and posts on social media, telling others that they've won cryptocurrency like Bitcoin or Dogecoin. Users will be asked to buy some crypto of their own and to send their wallet ID and private key to get the funds. After the wallet key is sent, they take all of the cryptocurrency out of the wallet.

4 **Phony Cash-Flipping Offers**

For this scam, someone tells you to send them a small amount of money and they will send you a larger amount in return (example: “send me \$10 and I’ll send you \$100”).

5 **Buying or Selling to a Stranger**

If you’re buying an item from a stranger, they might try to convince you to pay them before you receive the item. After you pay, the fraudster will start ghosting you without handing over what you purchased.

If you’re selling an item, the scammer could send fake emails pretending the payment went through or tell you that the payment will go through as soon as the item has been received. They also might use stolen credit cards or bank information, which could be flagged, and ultimately removed, from your account.

Ways to Avoid These Scams

→ **Say no to strangers.**

This is the first step to avoiding scams. Utilize the payment app’s security measures, like inputting the last four digits of a person’s phone number for the first time you pay them.

→ **Set yourself to private.**

While money apps may have become a new social platform, switching your account to private could help you better protect your wallet.

→ **Get notified.**

Turn on your notifications for all cash app devices, whether by text messages or emails, so you know when your account was used.





Double check representatives' legitimacy.

If you need to reach out to a representative of any of the payment apps, be sure you are speaking to someone who is truly with the company. Reach out only via the official website or app. If you receive an email from them, check that the sender is from a real company email.



Look for the checkmark on social media.

Most payment apps do host real giveaways on social media, where you could actually win money. To ensure you're not participating in a scam, look on the account that is running the giveaway and look for the checkmark next to the name.



Mark payments as a purchase.

If you are buying something from a stranger on Venmo, look on their account to see if they are an official business. If they are, it will say "Eligible items covered by Purchase Protection" under the pay button. And if you are buying an item from a personal profile, you can mark the item as a purchase for better protection.



HELPFUL TIP

If you think you or your child has been scammed using a payment app, reach out to the official app customer support, cut off communication with the scammer, and change your passwords as soon as possible.

Don't be afraid to use these apps, just be smart when doing so! For more resources on helping kids navigate finances, visit the Pelican State Credit Union Project ACCOUNTability website at ProjectACCOUNTability.com.



PROJECT
ACCOUNT*ability*

by Pelican State