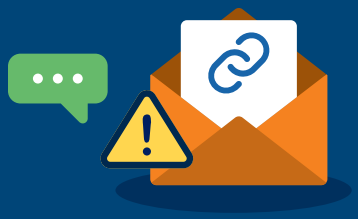
How to Safely Use Mobile Payment Apps and Services

Online payment systems or apps like Zelle, Venmo, and CashApp let you quickly send and receive money. If you link the service to your bank account or debit card, it's almost like handing someone cash. Be sure you know who you're sending money to. Once you send money, it's nearly impossible to get it back.

AVOID SENDING MONEY TO A SCAMMER



Don't click on links in an unexpected email, text message, or direct message that asks you to send money. Don't give any personal or sensitive information like your username, PIN, or password.

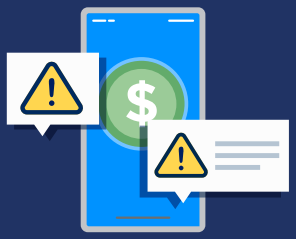
Confirm that you know the person you're sending money to.

When sending to someone you know, **double-check their information** before you hit send.

PROTECT YOUR ACCOUNTS

Use multi-factor authentication. This means you need two or more credentials to get into your account: your password plus something else like an authentication code or fingerprint.

Never share your credentials, like a verification code you get via text or authentication app.



Set up alerts in the payment app to get transaction notifications outside of the app environment, such as via email or text.

Regularly check your payment app and bank accounts to make sure no unauthorized payments have been sent from or accepted by your account.

Paid a Scammer Through a Payment App?

- **Report it to the payment app or service and ask to reverse the transfer.**
- **Tell your financial institution.**
- **Report it to the Federal Trade Commission at ReportFraud.ftc.gov.**

Learn more at **ftc.gov/paymentapps** and **aba.com/consumers**

ABA FOUNDATION®