Phishing Red Flags

Every day, money is lost to online phishing scams. Learn how to spot shady emails, phone calls and texts by knowing the things no bank would ever ask.

keen BANK

MOBILE PAYMENT APP SCAMS

Scams using payment apps such as Cash App, PayPal, Venmo or Zelle®, are one the rise as growing platforms become increasingly popular. It only takes seconds for a scammer to access your money.

Be wary of texts or calls about payment apps

Payment app scams often start with a phone call or text. If you get an unexpected call, just hang up. If you get an unexpected text, delete it. Even when they seem legitimate, you should always verify by calling your bank or payment app's customer service number.

Use payment apps to pay friends and family only

Don't send money to someone you don't know or have never met in person. These payment apps are just like handing cash to someone.

Raise the alarm on urgent payment requests

Scammers rely on creating a sense of urgency to get you to act without thinking. They might claim your account is in danger of being closed or threaten you with legal action. These high pressure tactics are red flags of a scam.

Avoid unusual payment methods

Banks will never ask you to pay bills using a payment app or ask you to send money to yourself. Scammers can "spoof" email addresses and phone numbers on caller ID to look like they're from your bank, even when they're not. When in doubt, reach out to your bank directly.

What to do if you get scammed on a payment app

1. Notify the payment app platform directly and ask them to reverse the charge.
2. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank.
3. If you have lost money, file a report with the local police department.
4. File a complaint with the Federal Trade Commission or call 877.382.4357.