New crypto payment scam alert

January 10, 2022
by
Cristina Miranda
Division of Consumer and Business Education, FTC

There's a new spin on scammers asking people to pay with cryptocurrency. It involves an impersonator, a QR code, and a trip to a store (directed by a scammer on the phone) to send your money to them through a cryptocurrency ATM.

It works like this: someone might call pretending to be from the government, law enforcement, or a local utility company. Maybe a romantic interest you met online calls, or someone calls to say you've won the lottery or a prize. They'll wind up asking you for money. If you believe the story they tell and you seem willing to engage, they'll stay on the phone to direct you to withdraw money from your bank, investment, or retirement accounts. Then they'll tell you to go to a store with a cryptocurrency ATM (and they'll stay on the phone the whole time). Once you're there, they'll direct you to insert your money into the ATM and buy cryptocurrency. Here's where the QR code comes in: they send you a QR code with their address embedded in it. Once you buy the cryptocurrency, they have you scan the code so the money gets transferred to them. But then your money is gone.

Here's the main thing to know: nobody from the government, law enforcement, utility company, or prize promoter will ever tell you to pay them with cryptocurrency. If someone does, it's a scam, every time. Any unexpected tweet, text, email, call, or social media message — particularly from someone you don't know — asking you to pay them in advance for something, including with cryptocurrency, is a scam.

If you spot something like this, tell the FTC right away at ReportFraud.ftc.gov. And to learn more about avoiding cryptocurrency scams, visit ftc.gov/cryptocurrency.