Send Yourself Money? That's a Big Red Flag

Scammers are always creating new ways to steal your money. One of the recent scams utilizing peer-to-peer payment services is what's known as the "Pay Yourself Scam."

The gist of the scam is that someone pretending to be a representative from your bank or credit union tells you that there has been a fraudulent transaction and in order to stop it, you need to send yourself money with Zelle®. That sense of urgency really works in their favor and gets unsuspecting consumers to act immediately.

The best way to avoid this scam is to know what to look for. Here's how it unfolds:

- It starts with a text message from a scammer that looks like a fraud alert from your bank or credit union. It's looks real and urgent!
- If you respond to the text message and engage the scammer, you'll receive a call from a number that may appear to be your bank or credit union.
- The scammer pretends to be calling from your bank or credit union and offers to stop the alleged fraud by directing you to send yourself money with Zelle®.
- In reality, the scammer is tricking you into sending money to their bank account.

How the Scam Works

So how are the scammers diverting money to their account?

When you enroll with Zelle® initially or if you switch your enrolled U.S. mobile number or email address to a different account, your bank sends you a security code to verify your identity. In this scam, the fraudster pretends to be calling from your bank or credit union saying that they need this passcode to authorize your payment to yourself. That should be a big red flag to you. Your bank will NEVER ask you for this security code, nor will they ask you to send money to yourself.

If the scammer gets the one-time passcode, they can link their bank account to your U.S. mobile number or email address. Now the money you thought you were sending to yourself is sent directly to their bank account.

- Never discuss account numbers, PINs or other personal information with anyone who contacts you, even if they say they are from your bank or credit union.
- If the person claiming a problem with your account needs your account information, hang up and call the bank yourself.
- Don't call the number in a text, email or voice mail. It will connect you directly with the scammers. Always look up the number online or review the number listed on your debit or credit card.

- Don't click on text message links from people you don't know, even if it’s pretending to be your bank or credit union. These links can be deceiving and direct you to a fraudulent site or expose your device to malware.
- Your bank or credit union will never ask you to send money to yourself (or anyone else)!

If you detect suspicious activity regarding Zelle®, hang up and contact your bank or credit union directly at the number listed on the back of your bank-issued debit card, in your banking app, or on their official website.

To learn about other scams and ways to protect yourself, visit zellepay.com/financial-education/pay-it-safe. To read about how you can report fraud and other related topics, visit stbank.com/security-center/.