PEER-TO-PEER (P2P) SCAMS
IS THERE MYSTERY MONEY WAITING FOR YOU?

November 2022 | Issue 2022:9

ZERO TRUST/PHISHING

The zero-trust philosophy is "never trust, always verify." Traditionally, this term is used when referring to computer network security. As this newsletter explains, adopting a zero- trust view when using P2P payment systems is a wise move.

Why are these scams so effective?
It's the combination of social engineering and phishing. The bad guys are creating a scenario where the consumer is confronted with the possibility that their bank account has been hacked. Immediately concerned, the consumer is more open to offers of assistance, aka, social engineering.

These four tips will help you to use P2P payments systems more securely.

-Only send or receive money from people you know personally.

-Confirm that you're transacting with the correct person by verifying the phone number. Anyone could impersonate someone you know changing their name and photo.

-Be cautious about using these apps to receive payment for goods or services.

-Call the P2P company's customer service directly to resolve erroneous transactions and do not send money to strangers.

Solomon Adote
Chief Security Officer

PEER-TO-PEER SCAMS ABOUND

If you use a peer-to-peer (P2P) payment systems like Zelle®, or Venmo, you appreciate the convenience and have confidence in the platform. Someone surely is taking care of security. You're not about to let a stranger change your password or send money to a totally random person.

According to Old National Bank, in one of the latest P2P scams, that's exactly what fraudsters are getting people to do. Learn how this scam works:

You get a text asking if you recently sent $XX dollars via Zelle® (or another platform) to a person you don't recognize. The text may look like it's coming from your bank. You respond "No," because you didn't. Next, your phone rings. The caller's identity is spoofed to be your bank. You pick up the phone and feel relief – this person is going to help you resolve this unauthorized P2P payment.

Of course, in reality, you never made any such payment. A fraudster is on the other end. They're trying to trick you into giving them your account info, so they can log in as you and pay themselves.

One way is the scammer asks for your online Username. You tell them and get a text that has a six- digit code. The fraudster wants that code to "complete the verification." In reality, that's your password reset confirmation. The criminals can now create a new password for your account, login as you, and send themselves money.

Another scam is " **Mystery Money**." With this, a stranger "accidentally" sends you money, then asks you to send them the money back. The problem is: the scammer added the money to their account using a stolen credit card or bank account, so Venmo (or whichever P2P you used) will flag the transaction as fraud eventually. Then, Venmo will take those funds out of your account, or, if you've already sent the money back to the sender, hold you responsible for that amount (and potentially block your account too).

When it comes to your P2P credentials, those are yours and yours alone. Your financial institution will not ask you to provide your passwords or codes or ask you to do anything as unorthodox as "pay yourself." It is best to use P2P payments only with people you know and trust. Another way to protect your payments is to link your credit card to the app and fund your payments through the credit card. When you do that, you could benefit from the same purchase protections that your credit card offers.