



PENNSYLVANIA STATE POLICE

COMMUNITY AWARENESS BULLETIN

CAB 003-21

December 13, 2021

THE "ZELLE SCAM"

The Pennsylvania State Police (PSP) is reminding Pennsylvania residents to be vigilant about scams involving peer-to-peer payment applications (apps) like Zelle, Venmo, and Cashapp. The PSP is aware of a scam specifically involving Zelle, a service offered by many financial institutions through the institution's mobile app that allows people to send money to customers of other banks.

In this scam, the fraudster sends a text message claiming to be from a bank's fraud department stating the victim had a suspicious payment through Zelle and asking the victim to verify the transfer. If the victim responds to the text, the fraudster calls the victim claiming to be from the bank's fraud department and asks for the victim's username to "verify their identity." The fraudster asks for additional information, including notifying the victim that they will be receiving a one-time code to their phone and a possible notification from Zelle about a transfer that has either just occurred or has occurred in the past. These are legitimately from the bank and from Zelle, but the fraudster knows about them, will tell the victim to expect them, and will ask the victim for the information to "verify" it. What the fraudster is actually doing is walking the victim through the process to reset the victim's account password. Once the password has been reset, the fraudster can empty the victim's bank account in a matter of minutes.

RECOMMENDATIONS

- Become familiar with your peer-to-peer payment app's policies related to fraud protection.
- Learn how to use your institution's mobile app and disable features you do not intend to use. Ask someone at your financial institution for help if needed.
- Learn to recognize your financial institution's fraud notifications and what you should do if you receive one.
- Read text messages closely and ignore those from institutions where you do not have accounts or that do not make sense.
- If you receive a telephone call from someone claiming to be from your financial institution, hang up and call them back at a phone number you know is valid. You can find the number online or in their mobile app.
- Login information, such as usernames, passwords, and any one-time codes or other authentication information, is confidential and should not be shared with anyone, including anyone from your financial institution. No one from your financial institution will ever ask for your login information.

PSP reminds residents who fall victim to a scam to report it to their local police department.