The RED FLAGS of Phishing Payment App Scams

- **Unexpected Requests:** Be cautious if you receive unexpected requests from strangers or organizations asking you to send money through a payment app. This is a scammer move.
- **Sending Money to Yourself:** If someone who claims to be your bank says you have to send money to yourself, you can be 100% certain it's a scam. Banks never ask that. Use payment apps to pay friends and family only.
- **Overpayment Claims:** Be skeptical if a sender claims to have accidentally overpaid you through Zelle® and requests a refund of the excess amount. Scammers use this tactic to trick you into sending them money.
- **Suspicious Links:** If you receive a payment app-related message that contains a link, never click it. Scammers often send links to fake login pages to steal your username and password.
- **Pressure and Urgency:** Scammers attempt to trick you by creating a sense of urgency. If they mention unforeseen emergencies, unverified transactions, account suspension, or unsolicited prize winnings, it's a scam.