



## Beware of P2P Fraud: How to Stay Safe When Using Payment Apps

Peer-to-peer (P2P) payment apps like Zelle, Venmo, and CashApp have made sending money as simple as sending a text message. Whether you're splitting the bill, paying your part of the rent, or sending a gift, P2P apps provide a fast and convenient way to handle transactions. However, with this convenience comes risk – scammers have found ways to exploit these platforms. It's crucial to understand the dangers and how to protect yourself from P2P fraud.

**What is P2P Fraud?** P2P fraud refers to any scam that involves tricking individuals into sending money via peer-to-peer payment platforms. These scams often result in victims losing money, with very little chance of recovering it. Here are some common types of P2P fraud:

- **Fake Buyers or Sellers:** Scammers might pretend to sell products or services online, asking for payment through a P2P app. Once the payment is sent, the scammer disappears without delivering the promised goods or services.
- **Phishing Scams:** Fraudsters may send you an email or text that appears to be from your P2P payment app, asking you to "verify" your account or log in via a fake link. Once you provide your information, the scammer gains access to your account and funds.
- **Impersonation Scams:** Scammers might pretend to be someone you know – such as a family member or friend – in need of urgent help. They'll request money through a P2P platform, often asking for it to be sent immediately to resolve an "emergency."
- **Business Scams:** In this type of scam, fraudsters pose as legitimate businesses or investors, pressuring victims into making a payment for a fake investment or service. Once the payment is made, the scammer vanishes.

**How to Stay Safe When Using P2P Payment Apps** While P2P apps are incredibly useful, it's important to take precautions to avoid falling victim to fraud. Here are some tips to help you stay safe:

- **Only Send Money to People You Know:** P2P apps are designed for transactions between people who know and trust each other. If you're buying from an unfamiliar seller or paying for something online, use a more secure payment method that will offer fraud protection.
- **Verify Before You Send:** If you receive an urgent request for money from a friend or family member, confirm it through a phone call or other direct communication. Scammers often create fake emergencies to get you to act quickly.
- **Watch Out for Phishing Attempts:** Never click on links in unsolicited emails or texts claiming to be from your P2P app. Always log into your account directly from the app or website itself to avoid phishing scams.
- **Enable Security Features:** Most P2P apps offer additional security such as PINs, multi-factor authentication (MFA), or biometric logins (like fingerprint or facial recognition). Enable these features to add an extra layer of protection to your account.
- **Monitor Your Account Regularly:** Check your P2P app account regularly for any unauthorized transactions. If you notice anything suspicious, report it to your bank or the app's customer support immediately.