NEW INTERNET SCAMS: A GUIDE FOR 2021-22

Presented by the Coastal Bend College Police Department

GAMERS AND PEER-TO-PEER PAYMENTS

- 58 percent of gamers
- 42 percent of people who use peer-to-peer payment apps

have been scammed in some way

CRYPTOCURRENCY

- ABOUT **1 IN 3** PEOPLE
  WHO USE CRYPTOCURRENCY EXPERIENCED
  SOME FORM OF SCAMMING ACTIVITY.
- MANY LOST MONEY WHEN PUTTING THEIR
  CRYPTO INTO A BAD EXCHANGE.

PEER-TO-PEER PAYMENTS

Peer-to-peer payments allow users to transfer funds between two people using websites or mobile apps. Popular peer-to-peer payment apps include Venmo, Zelle, PayPal and Cash App.

Scamming can occur across all peer-to-peer payment platforms. Users can be especially susceptible to scammers because if they authorize payments or money transfers, it’s their responsibility to ensure that the transaction is legitimate.

WHICH OF THESE SITUATIONS HAS HAPPENED TO YOU WHEN USING PEER-TO-PEER PAYMENT APPS?

- I paid for something and did not receive the product/service 23%
- I sent money to the wrong person and never got the money back 14%
- Scammers asked for my payment authentication codes for transaction 13%
- I clicked a text/email with fake customer support information 13%
- I was sent a payment that was later reversed because the original Funds were stolen 12%

HERE ARE SOME COMMON SCAMS ON A FEW POPULAR PEER-TO-PEER PAYMENT APPS:

ZELLE

- According to Zelle’s website, common scams on this payment app include advertisements of enticing offerings of everything from puppies to concert tickets.
- If you’ve paid for services or products and haven’t received what you paid for, you should report the loss to your financial institution immediately.

CASH APP

- Scammers often impersonate **Cash App** support members or service representatives who require sign-in codes or PINs.
- However, the app's service line is automated, so if you're talking to a human who asks for a sign-in code, **they are a fraudster.**
- Last year, a landlord from Raleigh, North Carolina learned that lesson the hard way after a fake service representative scammed him of $24,000, promising to help him transfer his **Cash App** money into his bank account.

- PayPal users are often scammed when they receive **phishing emails** that appear to be from PayPal, asking to verify their login information. Typically, these emails include links that mirror the real PayPal website.
- You should never verify your login information via email or give away your login information to strangers, even if the emails and links look legitimate.

PAYPAL

- Of those who lost money on peer-to-peer payment apps, the majority, (64 percent) lost it on **PayPal**.

Click to add text

- That’s likely because **PayPal**, which also owns **Venmo**, is one of the most popular peer-to-peer payment apps.

TIP

Never give anyone your Cash App sign-in code or PIN.

If someone is asking for it, **they're a fraudster**. **Never** give away your PayPal or Venmo information to strangers and ***don't verify your login information via email.***

CRYPTOCURRENCY INVESTMENT SCAMS

- **Cryptocurrency** (“crypto” for short) is an unregulated, global, and digital currency that takes the form of “coins” or tokens. A few examples of cryptocurrencies are **Bitcoin, Ethereum,** and **Litecoin**.
- While investors of crypto appreciate a global currency that isn’t regulated, by that same token, crypto investors are more susceptible to scams and fraud.

PREVENTING CRYPTO SCAMS

As with most scams, be wary of any unsolicited questions or calls about your investments and never give away your account information.

BE AWARE

- If someone asks you to pay upfront in crypto for the right to enter into a crypto pyramid scheme or a program that rewards you for actively recruiting others
- If crypto “investors” offer unsolicited services that include growing your accounts so long as you give them account access
- If you are offered a job that includes recruiting cryptocurrency investors, or selling, converting, and mining cryptocurrency
- If you are asked to pay for a good or service using only cryptocurrency[6]

WHAT TO DO IF YOU THINK YOU'RE BEING SCAMMED

THE FEDERAL TRADE COMMISSION (FTC) RECOMMENDS YOU TAKE THE FOLLOWING STEPS IF YOU BELIEVE YOU OR ANY OF YOUR FAMILY MEMBERS HAVE BEEN SCAMMED.

OF COURSE, THESE STEPS SHOULD TAKE PLACE IN CONCURRENCE WITH REPORTING THE SCAM TO THE PROPER AUTHORITIES.

- If you gave away personal passwords or information:
- Change your passwords and make sure your new password is secure. Failure to do so could result in identity theft.
- Check your bills, bank account statements, and credit reports to check if someone is using your identity.
- If your Social Security card was lost or stolen, contact the Social Security Administration.

MORE INFORMATION ON SCAMS

- Scam Alerts | FTC Consumer Information https://www.consumer.ftc.gov/features/scam-alerts
- On the Internet — FBI - www.fbi.gov/scams-and-safety/on-the-internet