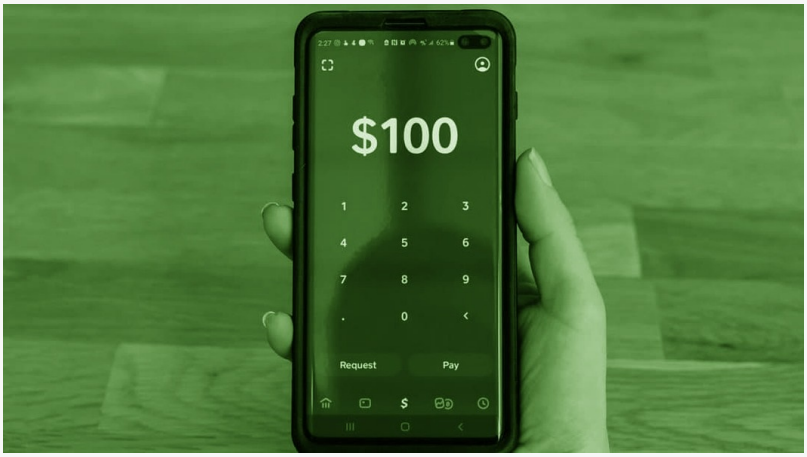
Cash App fraud: 10 common scams to watch out for



DUBAI, DUBAI, UNITED ARAB EMIRATES, August 8, 2022 /EINPresswire.com/ -- Phil Muncaster, guest writer at ESET highlights that it pays to be careful and here's how you can stay safe from fake giveaways, money flipping scams and other cons that fraudsters use to trick payment app users out of their hard-earned cash

For today's consumers, convenience is king. And at the heart of the digital experiences that make our lives easier sits the smartphone. Over the years, these devices have become an extension of ourselves, slowly replacing our cameras, our PCs and now our wallets.

But the popularity of the apps we use every day has made them an attractive target for fraudsters. And mobile payment apps like Cash App, Zelle or Venmo that allow users to send each other money are right at the top of their priority list.

The rise of Cash App

Cash App is used by tens of millions of people each month, especially because among other things, the app allows users to send and receive money instantly. Although it includes multiple features including PIN and biometric authentication, account usage alerts and a certain amount of protection from unauthorized charges, it can't insulate you from fraud. In short, if you're tricked into sending a fraudster money, that cash is most likely gone, never to return.

Understanding exactly what these scams might look like is the first step towards staying safe.

Top 10 Cash App scams

1. Super Cash App Friday impersonators
The weekly cash giveaway event on the platform's Instagram and Twitter accounts has,

predictably, been hijacked by fraudsters. They'll contact a participant via social media, tell them they've won and then request a fee in order to release the funds.

2. Cash flipping
The Cash App Friday/$Cashtag scam is sometimes a premise for another increasingly common type of fraud leveraging the service. Users are contacted saying that if they send a specific amount of money, they will be sent back more than the original amount. As most such offers are, this "cash flipping" deal is too good to be true.

3. Fake support
Scammers may set up fake support accounts on social media or use SEO poisoning to get fake websites featuring phony "Cash App support" phone numbers at the top of search results. When a user clicks through and rings up with a genuine complaint/request, they're asked for log-in info, enabling the fraudster to hijack and clear out their accounts.

4. Selling items online
Often, fraudsters try to sell non-existent items online – anything from a pure-breed puppy to tickets for a sold-out show. They might ask for a deposit, or even the whole amount, to be sent via Cash App. But unlike using a credit or debit card, there's no buyer protection for the victim.

In other examples, scammers may target online sellers, by sending fake payment notification screenshots and claiming the balance will only show up in the seller's Cash App account after delivery.

5. Phishing messages and vishing calls
Fraudsters also leverage the Cash App brand in classic email/SMS/phone-based social engineering efforts designed to trick victims into handing over their personal details. The aim, as in the fake support scams, is to get hold of information in order to hijack victims' accounts.

6. Fake Cash App receipts
Scammers claim that they've sent money to a victim's Cash App account by accident and ask them to return the amount. A spoofed receipt screenshot adds legitimacy to the request.

7. Debit card scams
Cash App also offers a debit card option for users. Scammers might use previously breached personal information to sign-up for one in a victim's name, and have it sent to their home. They'll request the recipient registers an app and scans a QR code to activate it. Such accounts could be used to launder funds from other scams.

8. Real estate rentals
In many cities across Europe and the US, rental property is in short supply. Scammers take advantage of this surging demand by reposting previously advertised apartments and homes, and requesting 'deposits' and 'application fees' via Cash App.

9. Romance scams
Romance scams resulted in losses of almost US$1 billion for victims last year, according to the FBI. Via fake profiles on dating sites, scammers will gain their victims' trust, pretend to 'fall in love' with them and then request money via Cash App for expenses such as plane tickets, medical treatment and more. In some cases, sugar daddy scammers, too, may ask their targets to make upfront payments using Cash App or another peer-to-peer payment app with the promise of receiving larger sums of money later.

10. Investment scams
This was another high-earning category of cybercrime, making nearly US$1.5 billion for scammers last year. Victims receive unsolicited emails/social media messages telling them about unbeatable (but fake) investment opportunities, often in cryptocurrency. As Cash App can be used legitimately to buy Bitcoin, it's a natural channel for crypto scams.

How to stay safe

The good news is that it shouldn't take much to keep the fraudsters at bay. By configuring the most secure settings in the app and treating any unsolicited contact with a healthy dose of skepticism, Cash App users can avoid most of the above scams. Consider the following:

Stay phishing aware: Never click on links or reply to unsolicited emails, texts or social media messages. Note that legitimate Cash App emails only come from @square.com, @squareup.com, or @cash.app. And the firm's support team will never request a sign-in code, PIN, Social Security Number (SSN), a payment or the downloading of a remote access app.

Optimize account security: Turn on two-factor authentication in any linked email account, switch on notifications in Cash App to track payments and ensure that a passcode is required when making any payment.

Secure your mobile device: Add a strong password or PIN and/or biometric authentication for lock-screen security.
Never send money to people you don't trust: Be skeptical of any requests – however small – for "deposits," payments in exchange for "free" cash and similar.

Minimize risk: Limit the amount of money stored in the Cash App account.

Don't Google Cash App support: Use the in-app chat function or these official channels suggested by the app.

In the event you may have been scammed, report it to Cash App. That way, the firm can try to recover your money or at least help to keep other users safe.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here