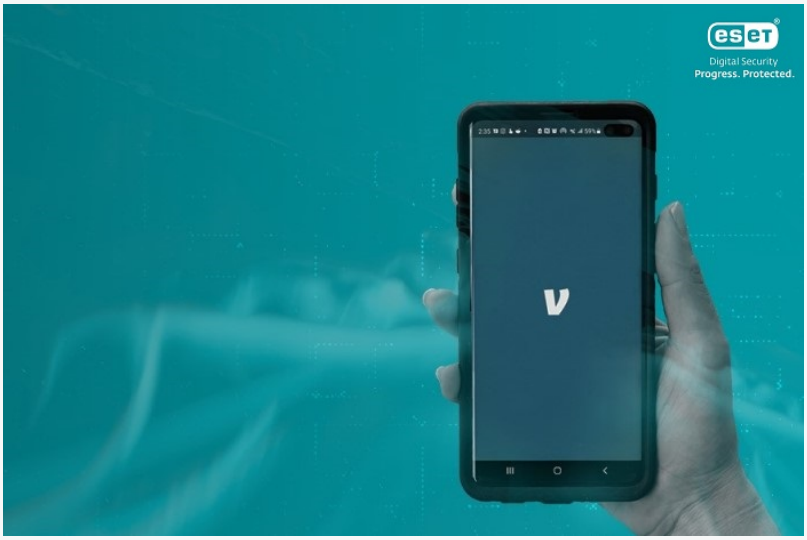
Top 10 Venmo scams – and how to stay safe



DUBAI, UNITED ARAB EMIRATES, January 18, 2023 /EINPresswire.com/ -- Phil Muncaster, guest writer at ESET explains that one does not have to be the next victim – here's what to know about some of the most common tricks that scammers use on the payment app

Today's consumers have a wealth of choice when it comes to paying and sending money online. A range of slick digital payment apps have emerged over recent years to make the whole process as seamless as possible for end users. But they're not the only ones who are winning.

Unfortunately, scammers have also found apps like Cash App, Zelle and Venmo to be fertile hunting grounds.

The story so far

Venmo began life back in 2009 as an SMS-based tool which gave its founders a handy way to send each other money, without having to use cash or checks. Now a part of PayPal, it's a fully-fledged digital wallet and payments service that allows users to send and receive funds quickly, easily and free of charge – via connected bank accounts. It processed an estimated US$230 billion globally in 2021.

However, unlike card payments, users aren't protected if they accidentally pay a fraudster. Once the money has been transferred, it's difficult to recoup. That makes it important for users to spot the warning signs of fraud before it's too late.

Common Venmo scams to watch out for

Venmo scams can take many forms. Some are linked to other fraud types like romance scams. Others might involve fake links, or attempts to steal not only money but also personal information. Here are among the 10 most common at the time of writing.

1. Fake prize/giveaway
A fraudster sends an unsolicited email or text message claiming the recipient has won money from Venmo. Sometimes they may be asked to take a fake survey in order to receive the winnings. Whatever the lure, the link attached to the message will usually take the victim to a phishing page designed to elicit personal and Venmo login details.

2. Purchase scams
For online buyers, especially those looking for items in high demand, there's also plenty to beware of. One of the simplest scams is for a fraudster to persuade the victim to send money (or part of it) without delivering the item in question. They may even share fake screenshots purporting to show the item has been delivered. The scammer might also ask the victim not to mark a payment as a purchase. Doing so will enable the victim to qualify for Purchase Protection if an item isn't delivered.

3. Payment error
The victim gets a note out of the blue from a stranger saying they have accidentally been paid. They will ask the victim to send the money back. However, the original money has usually been paid via stolen card details. So when the real cardholder finds out, they will request a chargeback and that money disappears from the victim's account.

4. Impersonation/money request
Fraudsters sometimes impersonate victims' friends, using info from their public feeds including profile pics, to make payment requests. They will usually add some kind of time pressure to force payment, such as pretending the friend has been caught out and about without any cash and urgently needs a quick Venmo payment.

5. Venmo phishing
In one variety, a fraudster manages to log into the victim's Venmo account, perhaps by buying their username and password from a dark web site. However, they can't get past the two-factor authentication (2FA) stage. That's why they'll call, pretending to be a member of the Venmo team and requesting that the user provides the MFA one-time passcode they will have received. The victim has just fallen prey to vishing.

Let's not forget about the classic phishing scam where the mark receives a notification out of the blue to say that there's a problem with their account and they need to act promptly to fix it.

6. Pyramid scheme/money circle/cash wheel
There are various names for this scam, but they all amount to the same thing. The victim receives an unsolicited offer claiming that if they send a small amount of money via Venmo, the scammer will "flip" it into a sum worth many times more and send it back. They may impersonate one of the victim's contacts to add legitimacy to the preposterous claim.

7. Fake payments

If users are trying to sell an item online, such as via Facebook Marketplace, scammers may try to use Venmo to trick them into believing a payment has already been made. This might include a fake screenshot purporting to confirm the payment. Or the scammer may pay using stolen card details, which means the payment is subsequently removed from the victim's Venmo account. They may even try to trick the victim by telling them the Venmo payment will only be confirmed once the item is sent, and shipping details uploaded to the app.

8. Check scam
A victim is trying to sell an item on an online marketplace. The scammer sends a check for more than the agreed sum, and then requests the extra be returned to them via Venmo. The check will usually bounce, meaning the victim is down the item and the money that they sent.

9. Tricks by bogus suitors and sugar daddies
Using fake profiles, romance scammers cultivate relationships with lonely hearts on dating sites, and then move the conversation on unpoliced channels like WhatsApp. After a few weeks of building trust and affection, they will usually request the victim sends them money for a made-up emergency, such as hospital bills or airline tickets. Fake sugar daddies or mommas have similar tricks up their sleeves, too.

10. Rental deposit scam
Scammers advertise properties for rent using scraped pictures and information. The property will usually be offered at a price far under the market rate, attracting numerous enquiries. The victims will be asked to pay a holding deposit via Venmo before they've even seen the place.

How to stay safe on Venmo
Venmo offers various security protections for its users, including data encryption, account monitoring, 2FA and account PIN codes. However, this doesn't always protect users from the fraud scenarios we've painted above.

Make sure to take the following precautions:

Only send and receive money from people you know and trust.
If you receive an odd request from someone you know, double check with that person to confirm the message was authentic.
Don't click on any links in unsolicited messages.
Keep Venmo transactions private so that they're visible only to the sender and recipient. To choose this option, one needs to go to 'Settings', tap on 'Privacy' and change the 'Default Privacy Settings' accordingly.
Choose a strong and unique password for your Venmo account and switch on 2FA.

Venmo also offers a contact form for users who have received a request they aren't sure about, and a mechanism to report suspected scams. Make sure to stay alert to fraud when using Venmo.

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