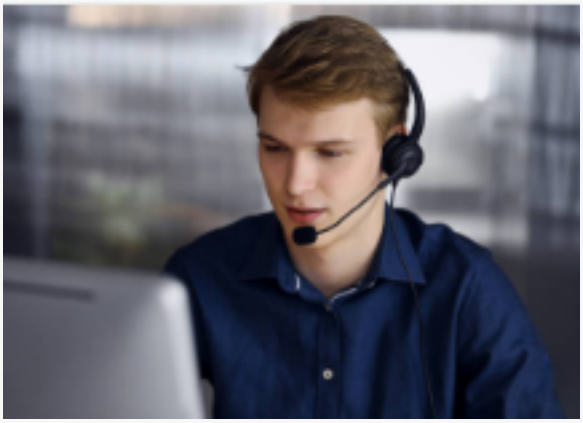
Cyber-Forensics.net explains online target hunting techniques: Suggests measures to avoid money payment app frauds

Cybercriminals have their eyes set on the money transfer apps. Look at the ways below to avoid becoming online scam victims.

Cyber-Forensics.net



Cyber Forensic Specialist

SOFIA, BULGARIA, March 1, 2022 /EINPresswire.com/ -- Cyber-Forensics.net is issuing urgent warnings as one-click-pay money transfer apps like CashApp, Zelle related scams are showing upticks in numbers of cases. The fraudsters are targeting app users and swindling millions of dollars.

Chief analyst Timothy Benson working at Cyber-Forensics.net, a cyber forensics service for online scam victims, says, "in most cases, scammers want the payment sent through Zelle, Venmo, or CashApp knowing they will receive the money before the victim finds out the order is fake."

Ideally, consumers need to report the matter within 24 hours to 72 hours of an incident to backtrace their payments. Usually, there is a small-time window that investigators can take advantage of to keep the victims' money from getting to scammers.

Another challenge is cutting into the time frame to determine if the payment made is fake. Since there are no universal ways to know when a scammer will liquidate the amount, Financial institutions can adopt additional security features to stay safe.

Special agent in charge, Peter Thompson working at the fund recovery company Cyber-Forensics.net, adds that mobile payments also make it harder to vet checks as they rely on the account numbers, and routing numbers-which can often be stolen from real accounts.

Ways Scammers Conduct their Online Scams Through Money Transfer Apps:

The “buy a pet with Zelle” scam:

> in most cases, scammers want the payment sent through Zelle, Venmo, or CashApp knowing they will receive the money before the victim finds out the order is fake."
>
> *Timothy Benson*

Pet scams shot up on the internet during the covid-19. However, virtual breeders did nothing but breed scams last year. They used stock photos of innocent puppies and kittens to lure victims. Once the thief successfully hooked the victim, they requested a deposit via Zelle to hold the new furry friend.

Maria Witrod was hit hard by Zelle scammers selling a nonexistent puppy. The thieves charged her nearly $1000 for the dog she thought she would have with her soon. However, the fake breeder asked for another $1000 to cover the shipping cost. Next came an additional request, so it went until Witrod ran out of money. With the scammer running away, Witrod learned a terrible lesson: never trust anyone online.

The Item for Sale scam:

Today, many online platforms are filled with online buyers looking to buy gifts online for loved ones. For the most part, consumer-to-consumer transactions are not regulated by any specific authority. Therefore, the rule of the land is "to beware online buyers and sellers scams online " because scammers might be on the hunt on those platforms.

A 34-year-old buyer Anthony fell victim to a scam via Twitter. Anthony was deeply hooked when a Twitter account holder told him he had won a chance to get a PlayStation 5. On asking how to get his reward, the scammer told Anthony to pay $549 via Zelle ASAP.

Determined to win the PlayStation 5, Anthony quickly completed the transaction. The scammer sent his victim a GIF of the grinch once he received the payment successfully.

Here is How to Use Payment Transfer Apps Carefully and Avoid Being Victims?

 Read the terms and use of the payment transfer apps carefully: It's vital to go through the terms and conditions of payment transfer apps like Zelle, PayPal, Western Union, etc., before downloading them and integrating them into banks. Even though the document is lengthy, please read it as the terms and use section can reveal eye-opening information about the operations.

 Only use official apps to send the money to friends and family: Never use payment transfer apps to buy pets, services. Strange web-based apps are vulnerable. And if required, ensure to check the recipient's name, number, or email correctly for payment. Account recovery specialist Peter Thompson added, "if the online user sent the amount by mistake, the banks might not facilitate a correction. Therefore, it depends on the stranger's willingness to return the sent

money. Therefore, it is necessary to use official applications to conduct transactions.

 Read all the prompts on the screen: After entering the friend and family members' contact information, websites usually prompt a confirmation request on the screen. Review all the messages carefully and match the appearing name on the screen.

Where to Report the Money Payment App Fraud?

If the app users have sent the money to scammers by mistake, they should immediately report the matter to the nearest mobile payment app center as used. Victims can also call bank authorities to stop their payment from going through

Trade Commissions: Then report the matter to Trade Commissions. Such services can use the information and build a case against scammers. For example, in the United States, the Federal Trade Commission is the agency that helps bring con artists to justice and put an end to the cybercrime that steals the money from potential targets through misleading business practices.

Fund Recovery Services: Victims can also hire fund recovery experts to increase their chances of recovering lost money. Fund recovery companies take little to no time to investigate the case and implement the best approach in recouping money from scammers through legal procedure.

About Cyber-Forensics.net

Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. Cyber-Forensics.net commonly deals with Bitcoin scams and Forex withdrawal problems. For more information, please visit https://cyber-forensics.net.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613
email us here
Visit us on social media:
Twitter