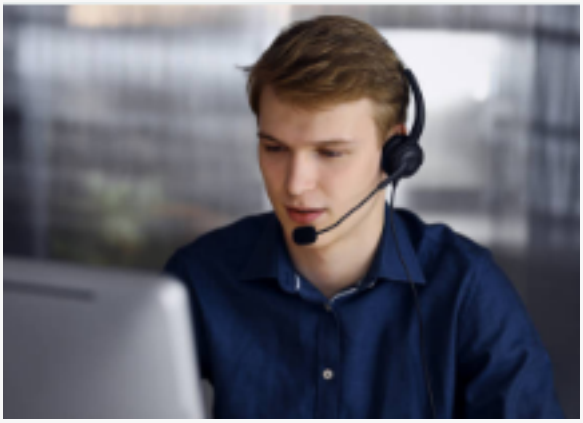
E-wallets become fertile ground for tricksters: Cyber expert Timothy Benson explains how to avoid online frauds

With just a single tap on the phone, e-wallets have revolutionized how users pay. However, e-wallets are also being adopted by fraudsters at a faster rate.

Cyber-Forensics.net



Cyber Forensic Specialist

SOFIA, BULGARIA, March 2, 2022 /EINPresswire.com/ -- Digital experts say that by 2025, more than half of the world's population is expected to use e-wallets. They are soaring high in popularity. Unfortunately, e-wallets have also become common grounds for hackers to launch frauds with a tendency to financially cripple users.

Fraudsters target e-wallet users because hacking into an e-wallet is easy and can earn cybercriminals a lot of money.

They contain bank details such as names, mobile numbers, and email addresses linked with the bank. Fraudsters who successfully get their hands on e-wallets end up gaining a lot more than just access to money. These criminals can even steal amounts and illegally manipulate consumer data.

Cyber-Forensics.net, a cyber forensics service for online scam victims, studied the emerging e-wallet frauds and explained many ways an e-wallet fraud actually happens:

How Do E-wallet Frauds Happen?

According to account recovery specialist Peter Thompson, there are several ways a fraudster can carry out an e-wallet fraud. Here is a closer look at some of the most common tactics tricksters may employ:

1. Abusing referral campaigns: Referral campaigns offer an easy way for e-wallet providers to bring in new customers. When users refer the payment channel to anyone, they receive back rewards as discounts or deals. But these incentives for users also mean incentives for fraudsters.

> e-wallet-frauds usually rely on misleading account users in making payments from individual bank accounts and get hold of their entire amount."
>
> *Timothy Benson*

The most interesting way referral abuse happens is through self-referrals. For instance, any e-wallet service runs a campaign offering $10 for every successful referral. A fraudster could create multiple fake accounts to rack up rewards and cause financial losses.

2. Using duplicate e-wallets: Duplicate e-wallets look identical to real ones. They are made to sound credible by uploading on app stores and posting fake positive reviews.

They may also upload images to lure users into believing they are legitimate. Once installed, the cyber thugs could use fake e-wallets to carry out various frauds such as stealing information and money or conducting internet attacks.

Gathering more information Peter Thompson investigated a similar case, which resonated with many users. Thousands of wallet users were told that their accounts were frozen. And to unfreeze the wallet, they had to transfer specific amounts of money.

He said, "e-wallet-frauds usually rely on misleading account users in making payments from individual bank accounts and get hold of their entire amount."

3. Taking control of real e-wallets associated with accounts: This problem occurs when fraudsters gain unauthorized access to accounts typically integrated with e-wallets. The thugs breach stolen credentials through social engineering schemes, phishing attacks, and available information online.

As a result, they also gain unauthorized access to valuable user information through e-wallets. This data can fetch high prices when sold online.

How to Avoid E-wallet Frauds?

E-wallet frauds can cause heavy damages and tend to repeat attacks to increase the scale of financial losses. Such scams also tend to hurt the bank-customer loyalty and brand reputation. It's essential to protect e-wallets and especially take protective measures. Down below are recommended tips by fund recovery service specialist Timothy Benson:

1) Enable additional security settings: Keep checking account settings to turn on additional security measures like multi-factor authentication options or using fingerprint recognition.
2) Link money transfers apps to credit cards: In many online purchasing cases, using a credit card helps protect consumers get the money back for failed goods and services and even claim money back from credit card companies.
3) Cancel unrequested transactions: Never follow any URLs sent by mistake. Users must be

careful when receiving emails from unknown people in the contact list Request the vendor to cancel the transaction as soon as possible. If the vendor refuses, the request is probably a fraud.
4) Use money transfers: To protect against fraud, try using money transfers apps to send funds to intended people.
5) Never enter a PIN, CVV, and OTP anywhere other than secured payment gateways.
6) Never transact using public wi-fi.
7) Ensure to visit the official websites for transactions.

What to do if Money is Lost in E-wallet Fraud?

Report the matter to financial institutions: Many financial organizations mandate users of mobile wallets to enjoy the same security as by regular credit cardholders. Report financial frauds to nearby trade commissions and local authorities.

Contact fund recovery experts: For legal advice on getting lost amounts back, contact fund recovery companies. These services may clarify what could be done in unauthorized, fraudulent transactions.

These days, digital wallet holders may be eligible for provision where financial institutions refund the entire amount if the complaint has been made within a specific period. At the same time, reporting fund recovery companies will help scam victims identify suspected criminals and suggest prevention techniques for the future.

How Do Fund Recovery Companies Help?

Over the past decade, customers have learned that breaching e-wallets have become easy for scammers. And once the scammers have access to these valuable e-wallets, they can easily place transactions and allocate funds to different accounts.

Fund recovery companies pave the way for recouping stolen funds by efficiently investigating the fraud's occurrence. Such firms are equipped with computer experts, law practitioners, ex-government agents who know all the ins and outs of how agencies operate. They ensure a smooth investigation flow, prepare documents, prove the fraud, and bring the criminals to justice.

Additionally, they provide tailored solutions and compile fund recovery reports against potential scammers. Companies that offer fund recovery services have the necessary skills and credentials to work with financial regulators and legal authorities. They receive the training to spot fraudulent activities and are well-versed with criminal behavior.

They understand the psychology of scamming tactics, extensive databases, and AI-powered technologies to track down the perpetrators.

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
