E-wallets now used to siphon money from debit, credit cards

V.Narayan@timesgroup.com

Mumbai: Long queues at ATMs and withdrawal limits on debit cards have prompted cyber scamsters to come up with a new modus operandi—using e-wallets to fraudulently siphon money from credit or debit cardholders. Experts say there are 50-50 chances of tracking the money once it is transferred to such e-wallets.

The fraudsters create several e-wallet accounts. "For a cashless society, security features should be good and cardholders should be more sensible while attending to such fraud calls," said investigators.

After demonetisation, police stations across the city registered 38 cases (from November 1 to December 12). The money was fraudulently transferred from the victims' cards to e-wallets. Cyber police said such cases are increasing as fraudsters, stumped by the withdrawal limits at banks and ATMs, have devised new means to obtain money. A cyber police officer said, "Initially, the fraudsters would transfer money

CRIME & THE CITY

fraudulently from a victim's card to an account and the money immediately withdrawn from some branch in Noida or Jharkhand or Gurgaon. Post-demonetisation, fraudsters are transferring money to multiple e-wallets. The wallets are created with a single mobile number (SIM procured through fake documents) money transferred in small amounts, ranging from Rs 4,000 but below Rs 20,000. Within seconds the money is transferred to e-wallets and spent online, before the bank or the police approach the e-wallet service provider to freeze the account."

Cyber expert Vijay Mukhi said e-wallets are basically apps on phones. "Most e-wallets do not do a KYC of the user, they simply use the mobile number. Most e-wallets do not even ask for an extra password while sending money to someone else," he said.

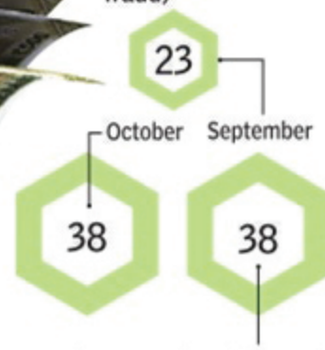
Another cyber expert Ritesh Bhatia said, "Post-demonetisation, many cases have come to me. The fraudsters can be traced with help from the bank and e-wallet service provider. But by then the damage is already done," said Bhatia.

Deputy commissioner of police (cyber) Sachin Patil said, "Never share your card or account details with a person who claims to be a bank executive. One should understand that banks never call anyone seeking details like OTP, card digits, account number, PIN etc. Awareness will be the biggest weapon to fight cyber crime."

NEW ELECTRONIC FRAUD METHOD

Credit/Debit Card Fraud Reported By Banks

FIRs Registered Over Fraud (e-wallet & cards) fraud)



E-wallet Fraud Cases Registered With Cyber Police In December: 2

HOW THE SCAMSTERS OPERATE

- Fraudsters posing as bank executives call the victim warning that his/her card is going to get blocked if he/she does not update their credit/debit card details
- Fraudsters alternately try to lure the victim with reward points
- They keep the victim engaged on phone seeking details, while they transfer money from the victim's credit or debit card to several e-wallets
- Fraudsters create several e-wallets using a single mobile number (SIM obtained through fake documents). They transfer money in the range of ₹5,000 to multiple e-wallets within seconds
- The e-wallet is used for online shopping, bill payments, etc
- Fraudsters started using e-wallets as after demonetization withdrawal limits have been set on debit/credit cards

ADVISORY

Do's | Set a password for your phone

- Set a password/pin for accessing the e-wallet
- Use anti-virus software
- Download app only from authorised application or sites that you can trust
- Turn off your device's NFC/bluetooth/wi-fi signal

Dont's | Do not keep the phone unattended for a long time

- Do not provide your credentials on sites without https protocol
- Do not rely on free anti-virus software or trial versions
- Do not download app from unauthorised or unknown sources
- Do not pay for or on behalf of others