MODUS OPERANDI FOLLOWED BY THE FRAUDSTERS THROUGH INVESTMENT / PART-TIME JOB / PONZI SCHEMES AND THE PRECAUTIONARY MEASURES

Online Scams

Fraudsters send attractive offers through letters, e-mails, calls, SMS messages asking you to deposit money to participate in schemes that "sound too good to be true". Later, they withdraw the money and stop further communication.

Here is a list of the most common frauds:

• Contests and lotteries that you had not registered for, asking you to make a payment for receiving your prize

• Emails appearing to have been sent from large corporations, public institutions and regulatory bodies

• Phone calls or SMSes offering jobs that you had not applied for; intimations of gifts or inheritances supposed to originate from a foreign country, asking you for personal information

• High-yield investment plans and multi-level marketing schemes offering unealistic returns on investment; please checks the credentials of the person offering these

Ponzi Scam

A Ponzi scheme attracts investors by offering guaranteed and unusually high returns, based on short-term and often complex investments. However, the underlying investments don’t exist. Returns are paid to the initial investors from the funds of subsequent investors, rather than from any actual profit earned. The perpetuation of the scheme requires a continued stream of money from new investors. Tips to avoid a Ponzi scheme:

• Beware of claims of guaranteed investments with above average returns

• Ensure that you receive detailed written information to fully understand and assess the underlying investment details

• Assess the promoter of the investment and do your homework, i.e. background check, whether they are licensed to sell securities - if they claim they are exempt, check with the local regulator

• If you have already invested and you are pressured to reinvest your returns, or there is a disruption of services by the promoter, contact the local regulator

• Consult an unbiased third party—like an unconnected broker or licensed financial advisor—before investing

• Always deal with a SEBI registered or authorised intermediaries, only

• Although many investment transactions are conducted by phone or online, be cautious about investment companies without established premises or offices

• Do not respond to unsolicited e-mails about investments, job offers or any requests for personal information without independently verifying the contents of the e-mail or phone call

• Avoid investments you are uncomfortable with, or don't understand

• Be vary of "get-rich-quick" offers and "hot tips"— you may stand to lose much more than you'll gain.

Investment scams

Fraudsters may impersonate Stock Broking Firms, Online Trading Advisors, or misuse reputed organisation names & logos to gain your trust towards investments.

How does this fraud happen?

Method 1

The fraudster will share attractive advertisements through a social media platform about free online trading tips or investment schemes with unusually high returns/profits in a short period of time!

Once you connect with the fraudster, they will first add you to a WhatsApp/Telegram group, and then convince you to make a payment to their account for the particular investment, or they will share a fraudulent link/app to proceed with the payment.

The fraudster will also send you a fake link/website which displays high returns for your invested amount and advise you to keep making such payments for investments.

Once you stop making the payments and request for withdrawal of invested amount and the profits, they will disappear by blocking your social media account & switch off their contact number. It’s now that you realise that it was actually an investment fraud.

Method 2

You will receive phishing calls from unknown people with regards to investments. The fraudster will ask you to download a screen sharing app and make a payment of Rs. 1 or 5 for registration/verification purpose. Through screen sharing apps, the fraudster may get access to your mobile device and may compromise your account credentials.

The fraudster can now view the UPI PIN inputted by you. They will now link your account through the UPI app and with the help of UPI PIN, carry out subsequent unauthorised transactions.

Extortion Scams

Extortion e-mails are a type of scam, where cybercriminals send threatening messages to individuals or organisations demanding payment in exchange for not releasing sensitive or embarrassing information. These e-mails typically claim that the sender has compromising information, such as private photos or personal data and threaten to share it with the recipient's friends, family or the public unless a payment is made.

The goal of these e-mails is to scare the recipient into paying the demanded amount, even though there might not be any compromising information to release.

Warning signs that it might be a scam

• You receive a call, message or e-mail unexpectedly from someone claiming to be from a government department, debt collection agency or trusted company.

• They will claim that you owe money and threaten you with legal action or arrest

• The caller will tell you that to fix the matter, you will need to pay a fee or fine

• The caller may ask for your personal information, such as your passport details, date of birth or bank information

• The caller may claim that the police will come to your doorstep and arrest you if you do not pay the fee or fine right away

• You may be asked to transfer money to an account to 'keep it safe' or for 'further investigation'.

Steps you can take to protect yourself

- Don't be pressured by a threatening caller asking for money. Hang up and don't respond
- Don't pay anyone by unusual methods such as gifts, hampers, vouchers or wire transfers
- Don't use any contact details provided by the caller. Verify their identity by calling the relevant organisation directly. Go to the organisation's official website and search for the contact details
- Do not respond to texts or e-mails. If you do, the scammers will increase their extortion attempts to get your money.
- Do not trust investment schemes assuring unusual high returns/profits that sound too good to be true.
- Refrain from clicking suspicious links/advertisements from unknown sources.

- Do not trust unsolicited investment schemes received on social media.
- Refrain from dealing with unregulated financial entities operating on social media.
- Before investing, verify if it is a legitimate financial institution & governed by regulatory bodies through their official website.
- Do not share any sensitive details like OTP, CVV, PIN, etc with anyone.
- Do not click on any unknown link or install any unknown app or link.
- Do not accept the messages as genuine simply because they name well-known companies.
- Any person that asks you to pay an amount upfront should be ignored and/or reported to the right authorities.

Additional safety tips

- Never send money or give credit card, online account details or identity information like your driver's licence or passport to anyone you don't know or trust. Never share them by e-mail or over the phone
- If you are concerned for your safety, contact the police
- If the scam is sent by e-mail, don't open any attachments, don't click on links and never download files. They can infect your computer with malware
- Report such incidents immediately to 1930 or cybercrime.gov.in
- To report a cybercrime to the police, dial the National Cybercrime Reporting Portal on 1930 or lodge a complaint through their website www.cybercrime.gov.in.