Formed
By AIBOC
In 2012

ALL INDIA BANK PENSIONERS' & RETIREES' CONFEDERATION
(A.I.B.P.A.R.C.)

Office of GS at:
4, Netaji Subhas Road,
1st Floor, Cubicle no: 170
KOLKATA– 700 001
Mobile: 9674188524, E-mail: aibparc2@gmail.com

Regd. Office:
MAYUR VIHAR, PHASE – 1
57 A, POCKET 3,
DELHI 110091

SENIOR OFFICE BEARERS:

PRESIDENT:

SHRI K. V. ACHARYA
MOB- 9868220338

GENERAL SECRETARY

SHRI SUPRITA SARKAR
MOB- 9674188524

WORKING PRESIDENTS:

1. SHRI C, GANGADHAR YADAV
MOB- 9440528806

2. SHRI P.S. PATKI
MOB- 8805607239

3. SHRI S.B.C. KARUNAKARAN
MOB- 9444772016

4. SHRI J.S. JAGADEESH
MOB- 9448508797

5. SHRI S. KUPPUSWAMI
MOB- 9444315928

6. SHRI S.C. AHUJA
MOB- 9650068773

7. SHRI ASOK DE
MOB- 9007513714

8. SHRI N.K. PAREEK
MOB- 9829015773

9. SHRI PAUL MUNDADAN
MOB- 9895378557

EXECUTIVE SENIOR VICE PRESIDENT:

SHRI HARVINDER SINGH
MOB: 9811353697

TREASURER:

SHRI TARUNESH CHATTERJEE
MOB- 9051601591

Circular no 144-26 **Date: November 22, 2026.**

For circulation among the members of the Governing Council, State Secretaries, Special invitees, Advisors, Affiliates, Constituents of CBPRO and members:

Dear Comrade,

Sub: <u>Vulnerability of the Senior and Super Senior citizens in the face of cyber crimes.</u>

1. Members are aware of the fact that the senior citizens of the country are very often becoming the victims of cyber crimes. Every day in newspaper, we find reports of the elder citizens being subjected to the evil designs of the fraud-makers. Our initiatives in this regard are well known. We wrote a detailed letter to the Chairman IBA citing various examples of how the senior citizens are suffering and what steps the Banks should take to protect the interest of the senior citizens. We do not know whether as per our request, IBA sent the copy of the letter to different Banks but we have been happy to note that immediately after writing the said letter, different Banks have started educative campaigns of different nature by sending messages and by giving advertisement in newspapers.

2. The fraud makers generally run at a faster speed and they go on inventing different modes to try upon the senior citizens. Very often in social media like Facebook and WhatsApp, different links are coming asking the senior citizens to apply for credit cards/debit cards or to submit the life certificate in a hassle-free manner. The senior citizens are being allured to be duped only. Keeping all such perils in mind, we decided to issue another advisory to our members to adopt highest degree of personal caution to protect his/her hard - earned money. We have taken the help of one of our members who retired from an important position of a Bank having a lot of theoretical and practical experience in this regard. We requested him to prepare the write – up in a very lucid language and also by avoiding technical jargons so that senior members can understand the contents clearly. At our request, he dealt with such cases only which have been reported in the public domain and we believe that the members will find the write –up as a helpful one.

It is given below:

Cyber fraud has been rising steadily, and senior citizens and pensioners are among its favourite targets. The reason is simple. We are known to have a regular pension, fixed deposits and the savings of a lifetime.

The person on the other end of the phone may claim to be a Bank Official, a police, CBI or ED officer, a telecom executive, a courier agent, an investment adviser, or even a relative. Often, he already knows your name, your mobile number and the bank you use. That tells you nothing about whether he is genuine. Most of these callers work in the same way. They frighten you, confuse you, tempt you or play on your feelings and they want you to act before you have had time to check. Even retired bankers have lost money this way. We request every member, and every spouse and family member, to read this note carefully and follow the precautions given below.

1. Fake pension, life certificate and KYC messages

Many pensioners have received messages saying things like these.

- Your pension verification is pending.
- Your life certificate has expired.
- Your KYC or PAN must be updated immediately.
- Your pension account will be blocked.
- Download this app to continue receiving your pension.

Such a message usually carries a link or an application file, often ending in .apk. Please do not install any app or APK file that reaches you through WhatsApp, SMS or email. A harmful app can read your messages, copy information from your phone and the criminals may misuse your banking facilities. For any pension, life certificate or KYC matter, go to your pension paying branch or use only the facility officially approved for the purpose.

2. Never hand over your unlocked phone to a stranger:

An elderly vegetable seller was recently approached by a man who said he was from her bank and had come to renew her KYC. She trusted him and gave him her unlocked phone. While pretending to help, he changed her digital payment settings. After that, her customers kept scanning her QR code and seeing the message "Payment Successful", but the money was going somewhere else and never reached her account.

Please do not let an unknown person handle your unlocked phone, whatever the reason given. That includes KYC, UPI, pension-verification, account-updating and so-called technical help. If someone says he represents your bank, confirm it with your branch yourself before you do anything.

3. There is no "digital arrest"

The caller may tell you that a parcel in your name has been found with drugs or other illegal items, that your Aadhaar or SIM card has been used in a crime, that your account is linked to money laundering, or that the police, CBI or ED are investigating you. On a video call you may even see a man in police uniform, and you may be shown what looks like an FIR, an arrest warrant or a court order.

You will then be told not to disconnect the call, not to tell your family, to move your money to a "safe account" for verification, and perhaps to break your fixed deposits for the purpose. Please do not do any of this. No genuine police officer, CBI or ED official or court will ever ask you over a phone or video call to transfer your savings to a safe account. Please cut the call, tell your family, and check the facts independently.

4. Do not break FDs, pledge gold or raise loans under pressure

A case reported from Karnataka shows how far this can go. A 62-year-old farmer was reportedly cheated of about Rs 1.31 crore by people posing as police and Anti-Terrorism Squad officers. They accused him of financing terrorism and threatened him with arrest. Frightened and under constant pressure, he is said to have closed fixed deposits held in his own name and his mother's, taken a loan against gold, mortgaged a commercial property and sent all the money to accounts named by the fraudsters. They told him to sit in a closed room, to tell no one, and to send a message every hour saying he was "safe and secure". They even told him to say, if the bank asked, that one transfer was for a house purchase for his daughter. It went on for weeks. He understood what had happened only when his daughter, having read a news report about another victim, warned him to be careful about such calls. He then told her everything and filed a police complaint.

Please remember the following.

• Never close an FD because someone threatens you with arrest or investigation.
• Never pledge gold, mortgage property or take a loan to meet such a demand.
• Never transfer money to any "safe account", "RBI account", "government account" or "verification account",
• Never give your bank a false reason for a transaction.
• Never keep such threats secret from your spouse, children or another person you trust.

If anyone asks you to lie to your bank or hide the matter from your family, take it as a clear sign of fraud.

5. The UPI rule everyone should remember

You never need to enter your UPI PIN to receive money. If someone asks you to scan a QR code and enter your PIN so that he can send you a payment-please refuse. Entering the PIN means you are allowing money to leave your account.

Be careful with UPI collect requests and Auto Pay mandates as well. A mandate can allow debits from your account in the future, so look through your UPI app from time to time for any mandate you do not recognise or no longer need.

6. Keep your secret banking details secret

Never tell anyone your OTP, ATM or debit card PIN, UPI PIN, CVV, or your internet and mobile banking passwords. No genuine bank employee needs them to protect your account. Please think of your OTP and PIN as the keys to your house. If a caller knows your name, your bank, your date of birth or a few account details, do not take that as proof that he is genuine. Such details are easy to buy or collect.

7. Unknown apps, links and remote access

Harmful apps and links come in many disguises. Some of the common ones are pension or life certificate verification, KYC or PAN update, traffic challan, electricity or gas bill, bank document, credit card update, courier notice, government scheme, reward or refund, and even a wedding invitation. Do not install unknown apps or APK files. Do not let a caller share your screen or operate your phone or computer from a distance.

8. SIM and e-SIM fraud

Someone may call in the name of your mobile company and ask you to upgrade your SIM or activate an e-SIM. If criminals get control of your number, your calls, SMS and banking OTPs can

reach them instead of you. If your phone suddenly loses network for no clear reason, do not just wait for it to return. Use another phone to contact your telecom provider and your bank at once.

9. A familiar voice or face can be faked

Artificial intelligence can now copy a voice and produce convincing fake audio and video. You may get a call that sounds exactly like your son or granddaughter saying " Papa, I have had an accident " or " Ma, the police have caught me, please send money now " Do not send anything in a hurry. Disconnect, and call the person back on the number already saved in your phone. It also helps if the family agrees on a secret code word to be used only in a real emergency.

10. Fake investments and easy money schemes

Be wary of WhatsApp and Telegram groups that promise guaranteed high returns, share market tips, assured IPO allotments, crypto currency profits, online trading opportunities or income from work at home. The fake app may show your money doubling or tripling, and you may even be allowed a small withdrawal early on so that you start trusting it. When you try to take out a larger sum, you will be asked to pay tax, a processing fee, a verification charge or an unlocking charge. Please do not send more money in order to get back money that is supposedly yours already.

11. Never lend your bank account

Someone may offer you a commission for letting money come into your account and then passing it on. Please refuse. That money is often stolen from fraud victims, and your account becomes a "mule account" for moving it. Do not lend, rent or sell your bank account, ATM card, SIM card or banking credentials. Your account can be frozen and you may have to face a police inquiry.

12. Other common traps

Be careful with unexpected messages and calls of the following kinds.

- Courier or customs. A parcel with illegal items has been found in your name.
- Electricity. Your connection will be cut tonight.
- Credit card. Your reward points expire today.
- Income tax. Your refund is ready.
- Lottery. You have won a prize.
- Loan. Instant loan without any documents.
- Online jobs. Earn money by liking videos or completing small tasks.
- Social media. A friend suddenly asks for urgent money.
- Customer care. A number picked up from an internet search may not be the real one.
- Friendship or matrimonial sites. An online acquaintance wins your trust and later asks for money.

Whatever the story, do not rush. Check first.

13. A simple safety plan for the family

Every member should name at least one trusted person in the family who can be consulted before any unusual or urgent payment. A good house rule is that no large or unusual payment is made without first speaking to one other trusted person. The Karnataka farmer was freed from the fraudsters only when a conversation with his daughter broke the secrecy they had imposed on him.

It is also wise to go through the following regularly.

- Bank statements and SMS alerts
- UPI transactions

- Newly added beneficiaries
- UPI and Auto Pay mandates
- Debit card and UPI transaction limits
- The mobile number and email registered with the bank

Keep sensible transaction limits, and as far as practicable do not hold a very large balance in the account you use every day for UPI. Never ignore an unexpected debit message, OTP, new beneficiary alert or Auto Pay notification.

14. If you have been unfortunately cheated:

Please do not feel ashamed. Sensible and experienced people are cheated too, and what matters now is speed. Call the National Cybercrime Helpline 1930 immediately. Then do the following.

- Inform your bank at once through its official channel and ask for blocking or other protective action.
- Report the fraud on the National Cybercrime Reporting Portal.
- Keep all SMS, WhatsApp messages, emails and screenshots, and do not delete anything.
- Note down transaction numbers, beneficiary accounts, UPI IDs and telephone numbers.
- If a suspicious app was installed, stop using that phone for banking until it has been checked.
- If your SIM suddenly stops working, contact your telecom provider from another phone.

The sooner you report, the better. Quick reporting can help in stopping the money from moving further. It does not guarantee recovery, but delay makes recovery much harder. You may also lodge your complaint on the National Cybercrime Reporting Portal.

15. A word to our members

We have all spent many years serving bank customers and looking after their money. That experience is valuable, but it does not make us safe from fraud. Today's fraudsters can be polite, convincing and well informed. They know banking procedures, they use official looking papers, and they may even say they are calling to protect your money. A caller who sounds knowledgeable or important is still a stranger.

Stop whenever someone creates fear, secrecy and urgency. Stop when someone asks you to move your money to keep it safe. Stop when someone asks you to hide the truth from your family or your bank. Then check with your bank or a trusted family member before doing anything else.

Stop. Check. Verify.

Fraudsters keep changing their methods, but what they want stays the same. They want you to act before you have time to think. However urgent the situation seems, take a few minutes and speak to someone you trust.

Members are requested to keep this advisory and to share it with their spouses, family members, fellow pensioners and other senior citizens.

We wish that the members will find the write–up useful for them.

With best wishes and regards,
Comradely yours,

K.V. Acharya.
President, AIBPARC
& Jt. Convenor, CBPRO

Suprita Sarkar
General Secretary