

PUBLIC NOTICE

CAUTION AGAINST FRAUDULENT SMS/CALLS E MAILS/ WEBSITES/ MOBILE APPS/ ADVERTISEMENTS/ CYBER ATTACKS



Unscrupulous individuals/entities are duping the general public by offering fraudulent schemes in the name of PFRDA/NPS/APY. These frauds are being perpetrated by advertisements/unsolicited advice through SMS, calls, websites, mobile apps, and social media platforms such as Facebook, WhatsApp, Telegram, etc.



PFRDA cautions the general public/ subscribers of NPS & APY who have been receiving spurious calls from unscrupulous individuals demanding large sums of money with the promise to release their corpus of funds in NPS/APY.



Fraudulent websites & Mobile applications spuriously referring to PFRDA/ NPS/ APY/ Retirement wealth/ Pension are falsely promising large sums of money as pension or unrealistic returns on periodic contributions being made to the accounts mentioned on the fraudulent websites & Mobile applications.



In light of perpetration of such frauds, PFRDA reiterates that it is a regulatory body regulating NPS and administering APY, NPS Lite, Swavalamban. PFRDA does not involve itself directly or through any representative to offer any scheme to any individual.



It is reiterated that PFRDA does not maintain the accounts of the subscribers or manages the release of funds directly, but administers accounts only through the intermediaries registered with the PFRDA for the purpose.



The only official Website of PFRDA is www.pfrda.org.in and the public are advised to be wary of phishing attempts by fake websites that replicate the official website closely with unnoticeable changes in the domain name.



On receiving SMS referring to PFRDA/ NPS/ APY/ Retirement wealth/ Pension etc., subscribers are requested to verify the sender prior to their response.



PFRDA only sends SMS with Sender ID – **PFRDAI**.



All the subscribers and the general public are hereby advised to maintain caution against such fraudulent and unscrupulous activities and are advised to exercise due diligence by following the best practices (Annexure 1) to protect themselves.



Kindly contact the Information desk for details on NPS and APY & Steps to be followed in case of cyber crime fraud are provided at Annexure II.

NPS Information Desk

Call Centre: 1800 110 708
SMS: **NPS** to 56677

APY Information Desk

Call Centre : 1800 110 069



Annexure 1

BEST PRACTICES TO PROTECT AGAINST FINANCIAL FRAUDS

Do not entertain spurious SMS/ Call/ E- mail / letter with unrealistic or false promises.

Do not share sensitive personal and financial details/ PRAN No./ Passwords with any individual/entity.

Exercise caution and perform due diligence when any individual/ entity offers unrealistic returns.

Do not transfer payment/ contribution to unauthorized individuals/ entities.

Use the official websites/ Mobile Application of PFRDA/ NPS Trust/ Intermediaries registered with PFRDA for activities pertaining to NPS/APY as applicable.

On noticing such fraudulent activities, members of the public are advised to lodge police complaint giving full details in the local police station.



STEPS TO BE FOLLOWED IN CASE OF FRAUD

1 DISCONNECT AND DETACH

- a. In case of an ongoing attack on your computer or IT infrastructure, your first step should be to disconnect the device from the Internet as this is the most effective way to prevent further loss of data.
- b. In the event of a phishing attack, where in personal and confidential information has been revealed do the following.
 - i. Freeze your bank accounts and credit cards
 - ii. Alter your Internet and mobile banking password.

2 INITIATION OF LEGAL ACTION

- a. Cyber Crime complaints may be registered on the **National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>**
 - i. The complainant shall initiate the filing of the cyber crime on the portal by registering with their name and Indian mobile number.
 - ii. An OTP (One Time Password) will be sent to the mobile number provided by the complainant which will be valid for 30 mins.
 - iii. After entering the OTP, the complainant will be successfully registered and can proceed with the complaint.
 - iv. In the complaints page, category and sub-category of the complaint may be chosen and details of the incident and suspect shall be provided.
 - v. Once the complaint is successfully registered, the complainant may download the PDF of the complaint from the portal and will receive confirmation on email and mobile no.
- b. Other alternatives for recourse against Cyber Crime:
 - i. The Cyber-crime complaints be registered with the cyber-crime cells either online/offline.
 - ii. It is not necessary for the victim to register the complaint in the cyber-crime cell of the city in which he or she is residing or where the crime was committed. For Example: Complaint against a fraud that occurred/originated in Delhi can also be filed with the cyber-crime cell in Mumbai.
 - iii. In case the victim does not have access to any of the cyber crime cells, he or she can lodge the FIR at the local police station under Section 154 of Code of Criminal Procedure.
- c. Alternately the National helpline no. 155260 may be contacted to register complaints on cyber fraud.