



Urgent Warning: Protect Yourself Against **KYC UPDATE AND CARD LINKING FRAUDS** Advice from **Telangana State Cyber Crime Bureau**

Cyber fraudsters are resorting to various tactics, including calls and SMS messages, to target individuals for fraudulent purposes:

1. They may claim to be from your bank, insisting on linking your Aadhaar number or PAN to your bank account, or updating your KYC details.
2. Alternatively, they might contact you under the pretext of replacing a card that is due to expire soon. They often use threats of deactivating your bank account or card if you fail to comply with their demands.



PRECAUTIONS TO TAKE

- Always exercise caution and verify any requests for KYC updates or linking of documents with your bank directly. Visit the official bank website or contact your Branch Manager to confirm the authenticity of such requests.

- Never disclose sensitive details of your credit or debit cards, including card numbers, expiry dates, or CVVs, especially over the phone or through web forms.

- Refrain from responding to unsolicited calls or messages requesting personal or financial information.

- When in doubt about the authenticity of bulk SMS messages or short codes supposedly sent by your bank, reach out to your branch manager for clarification and verification.

- Your safety and financial security are our top priorities. By staying vigilant and following these precautions, we can collectively combat KYC update and card linking frauds and protect ourselves and our community from falling victim to such malicious activities.

If you suspect that you have been targeted by fraudsters or have encountered any suspicious activity, please report it immediately to the **Telangana State Cyber Crime Bureau**.


Stay vigilant, stay safe.

Best regards,



Telangana State
Cyber Security Bureau

Reporting Portal  cybercrime.gov.in

Toll-free number  1930

Cyber fraud registry  8712672222