

Protect Your Biometric Data

User Safety Do's & Don'ts for Aadhaar and Biometric Authentication

Your biometric data is a sensitive personal identity credential. Unlike a password, many biometric characteristics cannot simply be changed if copied or misused.

Use your biometric data only when you understand and approve the transaction being performed.

DO's – Protect Your Biometric Data

1. Keep Your Aadhaar Biometrics Locked When Not Required

Use the official Aadhaar Biometric Lock/Unlock facility to keep your biometric data, iris and face biometrics locked when you are not actively using Aadhaar biometric authentication.

Temporarily unlock your biometrics only when you personally need to complete an authorised authentication.

Unlock → Authenticate → Lock Again

Watch the video to know how to do it -<https://www.youtube.com/shorts/WQ47pAoFu74>

2. Provide Your Biometric Data Only After Understanding the Transaction

Before placing your finger on any scanner, confirm:

- Why your biometric data is required
- Which service or transaction is being performed
- Which organisation is requesting authentication
- Whether you have authorised that transaction

Never scan first and ask questions later.

3. Check the Operator Screen Before Providing Your Biometric Data

Where the transaction information is visible, check the operator/device screen before placing your finger.

Make sure the displayed transaction corresponds to the service you requested.

If the screen shows a different customer, transaction, service or purpose:

DO NOT PLACE YOUR FINGER ON THE SCANNER.

4. Provide Your Biometric Data Only for the Transaction You Approved

One approved transaction should mean biometric capture only for that approved purpose.

Do not provide additional biometric captures for unrelated activities.

If another capture is requested, ask:

“Why is my biometric data required again?”

5. Verify the Result After Every Biometric Attempt

After placing your finger, check whether the authentication was:

- Successful
- Failed
- Cancelled
- Still pending

Do not immediately place your finger again without knowing what happened to the previous attempt.

6. Be Alert When Multiple Biometric Attempts Are Requested

A genuine biometric capture may occasionally fail because of finger condition, sensor quality, connectivity or other capture conditions.

However, if an operator repeatedly asks you to scan:

STOP → CHECK THE SCREEN → ASK THE REASON → VERIFY THE PREVIOUS RESULT

Do not continuously provide biometric captures without understanding why each retry is required.

7. Keep Your Biometric Data Under Your Control

Your finger should remain under **your control and supervision** throughout authentication.

Personally place your finger on the scanner.

Do not allow someone to repeatedly press, position or use your finger without explaining the transaction.

8. Use Only a Genuine Biometric Scanner

For Aadhaar authentication, provide your biometric data only through an authorised biometric authentication process and approved biometric device.

Be suspicious of unknown devices connected to:

- Personal laptops
- Unverified mobile phones
- Unknown applications
- Unauthorised websites
- Unrecognised POS terminals

9. Keep Your Finger Clean Before Authentication

Use a clean and reasonably dry finger.

Dust, excessive moisture, grease or dirt can cause genuine authentication failures and unnecessary repeated scanning.

10. Personally Observe the Biometric Capture

Remain present during the complete authentication.

Watch:

Transaction Selection → Biometric Capture → Result

Do not turn away while the operator changes applications, transactions or customer details.

11. Review Your Aadhaar Authentication History

Periodically review your Aadhaar Authentication History using official Aadhaar services.

Check for:

- Authentication you do not recognise
- Unexpected biometric transactions
- Unusual dates or times
- Unknown requesting organisations
- Repeated failed authentications

If you find a transaction you did not perform, investigate it promptly and report to authority with proof.

12. Lock Your Biometrics Immediately After Suspicious Activity

If you believe your biometric data may have been misused or an unknown authentication has occurred:

LOCK YOUR AADHAAR BIOMETRICS IMMEDIATELY

Then review your authentication history and report the suspicious transaction through the appropriate official channel.

Watch Video to know how do to -<https://www.youtube.com/shorts/WQ47pAoFu74>

13. Keep Your Registered Mobile Number Secure

Your registered mobile number is an important part of controlling Aadhaar services.

Keep your:

- Phone
- SIM
- OTPs
- Aadhaar account access

secure.

14. Use Virtual ID Where Appropriate

Where the service supports it, consider using Aadhaar Virtual ID instead of unnecessarily sharing your Aadhaar number.

15. Ask for the Purpose Before Giving Consent

Providing biometric data should never become a routine action without verification.

Before biometric authentication, know:

WHO is asking → WHY they need it → WHAT transaction is being authorised

DON'Ts – Never Do These

1. Never Provide or Reproduce Your Biometric Data on Paper for Digital Authentication

For Aadhaar or normal electronic biometric authentication, there should be no need to create a separate physical copy or representation of your biometric data.

Never unnecessarily provide your thumb impression or any other biometric representation on:

- Blank paper
- Loose sheets
- Cards
- Labels
- Forms unrelated to an authorised requirement

A physical biometric impression or representation can expose sensitive biometric information.

2. Never Reproduce Your Biometric Data Using Any Material

Do not create replicas, impressions or representations of biometric data using any other material

Your biometric data should be captured live through the authorised biometric device, not reproduced as an object or stored representation.

3. Never Allow Anyone to Make a Copy of Your Biometric Data

Do not cooperate with anyone who asks you to:

- Create a biometric mould or replica
- Make a copy or replica of your biometric pattern
- Provide a sample for “testing”
- Press your finger into unusual material
- Provide biometric impressions or samples for unauthorised device testing

unless it is part of a clearly authorised legal or official process.

4. Never Store Your Biometric Data as an Image

Do not intentionally photograph, scan or save your biometric data as:

- JPG
- PNG
- PDF
- Screenshot
- Scanned document
- Mobile image
- Computer file

Your biometric identity should not be treated like an ordinary photograph.

5. Never Keep Biometric Data Images in Your Phone Gallery

Avoid storing clear biometric images, including iris, facial or other biometric captures, in:

- Gallery
- Downloads
- Notes
- File manager
- Email
- Cloud drive

6. Never Send Your Biometric Data Through WhatsApp or Messaging Apps

Never send biometric impressions, biometric images or biometric capture files through:

- WhatsApp
- Telegram
- Email
- SMS/MMS
- Social media
- Chat applications

A genuine biometric authentication should not require you to send someone a photograph, image or file containing your biometric data.

7. Never Upload Your Biometric Data to an Unknown Website or App

Do not upload a biometric image or biometric data file to an unknown:

- Website
- Mobile application
- Registration form
- Testing portal

for “verification”.

8. Never Allow Someone to Photograph or Copy Your Biometric Data

Do not permit an operator or another person to photograph:

- Your thumb impression
- A biometric impression left on paper or another material
- A biometric capture displayed on screen
- A biometric capture image

without a legitimate and clearly explained requirement.

9. Never Share High-Resolution Close-Up Images of Your Fingertips

Avoid deliberately publishing high-resolution images that clearly expose biometric characteristics such as ridge patterns, iris details, facial geometry or other biometric identifiers.

Your biometric characteristics deserve the same level of protection as other sensitive identity credentials.

10. Never Provide Your Biometric Data Without Knowing the Purpose

If somebody says:

“Just put your finger here.”

Ask what transaction is being performed first.

Never provide biometric authentication simply because a scanner is placed in front of you.

11. Never Provide Biometric Data for a Blank or Unknown Transaction

Do not authenticate when:

- No transaction is shown
- The operator cannot explain the purpose
- Customer details are incorrect
- The amount/service is incorrect
- Another person's details are displayed
- The application appears suspicious

12. Never Continuously Scan After Multiple Failures

Do not provide biometric capture after biometric capture without checking what is happening.

After repeated failures:

STOP → CHECK → ASK → VERIFY

Repeated scanning should not become automatic.

13. Never Allow an Operator to Capture Your Biometric Data After the Transaction Is Complete

Once the authorised transaction has successfully finished, do not provide another biometric capture unless a separate legitimate transaction has been clearly explained and approved by you.

14. Never Allow Someone to Use Your Finger While You Are Distracted

Remain attentive during biometric authentication.

Do not allow biometric capture while you are:

- On a phone call
- Signing unrelated documents
- Looking away from the screen
- Completing another transaction

15. Never Leave Your Finger Resting on the Scanner

Place your finger only when instructed for the authorised capture and remove it once the capture is completed.

16. Never Use an Unknown Biometric Scanner or Capture Device

Do not provide your biometric data on an unidentified scanner or capture device simply because someone claims it is connected to Aadhaar.

Use only the approved authentication setup of the service you are intentionally accessing.

17. Never Allow Your Biometric Data to Be Captured Through Unauthorised Software

Do not authenticate through:

- Cracked applications
- Modified software
- Unknown browser extensions
- Unverified biometric applications
- Unofficial authentication tools

18. Never Try to Bypass an Authentication Failure

If genuine authentication fails, do not permit anyone to:

- Alter the scanner
- Use another unauthorised application
- Manipulate biometric data
- Use a stored biometric image or file
- Create or use a biometric replica
- Use suspicious third-party software

Contact authorised support or use an approved alternative authentication method where available.

19. Never Share Your Aadhaar OTP

An operator performing biometric authentication does not need unrestricted access to your OTPs.

Never disclose an OTP unless **you understand and approve the exact transaction for which it has been generated.**

20. Never Allow Someone Else to Authenticate on Your Behalf Using Your Finger

Your biometric data represents your identity.

Do not allow anyone to physically use your finger to authorise a transaction that you have not personally understood and approved.

21. Never Assume a Failed Scan Means “Nothing Happened”

A failed biometric authentication is still an authentication attempt.

If repeated failures occur, verify the reason rather than continuing blindly.

22. Never Ignore an Aadhaar Authentication You Do Not Recognise

If your authentication history contains a transaction you did not initiate:

DO NOT IGNORE IT.

Lock your biometrics and investigate the transaction.

STOP IMMEDIATELY IF YOU SEE THESE WARNING SIGNS

Do not provide your biometric data if someone:

- Cannot explain why your biometric data is required
- Refuses to show or explain the transaction
- Requests several biometric captures without explaining failures
- Asks you to make a biometric impression or replica on another material
- Wants to photograph or copy your biometric data
- Wants a biometric image or file sent through WhatsApp
- Wants to save your biometric data as a JPG/PDF or other file
- Uses an unknown biometric application
- Connects the scanner to suspicious software
- Asks you to authenticate another person's transaction
- Requests biometric capture after your transaction is already complete
- Attempts to distract you during authentication

If Multiple Biometric Attempts Occur

Follow the **STOP-CHECK-VERIFY** Rule

STOP

Do not continuously provide your biometric data.

CHECK

Look at the operator/device screen and confirm the transaction.

ASK

Ask why the previous authentication failed.

VERIFY

Confirm that another authentication attempt is genuinely required.

AUTHENTICATE

Provide your biometric data again only after you are satisfied.

Aadhaar Biometric Safety Rule

 LOCK →  TEMPORARILY UNLOCK →  AUTHENTICATE →  LOCK AGAIN

Keep Aadhaar biometrics locked when you do not require biometric authentication.

Temporarily unlock them when you personally intend to authenticate.

After completing the required authentication, lock them again for additional protection.

Watch Video how to do -<https://www.youtube.com/shorts/WQ47pAoFu74>

Remember

YOUR BIOMETRIC DATA IS PART OF YOUR IDENTITY. PROTECT IT LIKE A CREDENTIAL YOU CANNOT SIMPLY CHANGE.

Never copy it.

Never photograph it.

Never share it.

Never create a replica.

Never give it without knowing the transaction.

Never keep scanning without checking the result.

Use it only for a genuine, authorised and clearly understood transaction.