

PROTECT YOUR **BIOMETRIC DATA**

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

USER | ENGLISH + HINDI

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

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.

अपने बायोमेट्रिक डेटा की सुरक्षा करें

आधार और बायोमेट्रिक प्रमाणीकरण के लिए उपयोगकर्ता सुरक्षा: क्या करें और क्या न करें

आपका बायोमेट्रिक डेटा आपकी पहचान से जुड़ी संवेदनशील व्यक्तिगत जानकारी है। पासवर्ड के विपरीत, कई बायोमेट्रिक विशेषताओं को कॉपी या गलत उपयोग हो जाने के बाद आसानी से बदला नहीं जा सकता।

अपना बायोमेट्रिक डेटा केवल तभी दें जब आप समझते हों कि कौन-सा लेन-देन हो रहा है और आपने उसे स्वीकृति दी हो।

क्या करें - अपने बायोमेट्रिक डेटा की सुरक्षा करें

1. जब आवश्यकता न हो, अपने आधार बायोमेट्रिक्स को लॉक रखें

आधार बायोमेट्रिक प्रमाणीकरण की आवश्यकता न होने पर आधिकारिक Aadhaar Biometric Lock/Unlock सुविधा का उपयोग करके अपने फिंगरप्रिंट, आइरिस और फेस बायोमेट्रिक्स को लॉक रखें। केवल अधिकृत प्रमाणीकरण के समय उन्हें अस्थायी रूप से अनलॉक करें।

अनलॉक करें → प्रमाणीकरण करें → फिर से लॉक करें

कैसे करें, यह जानने के लिए वीडियो देखें: <https://www.youtube.com/shorts/WQ47pAoFu74>

2. लेन-देन समझने के बाद ही अपना बायोमेट्रिक डेटा दें

- स्कैनर पर उंगली रखने से पहले यह पुष्टि करें:
- आपका बायोमेट्रिक डेटा क्यों आवश्यक है
- कौन-सी सेवा या लेन-देन किया जा रहा है
- कौन-सी संस्था प्रमाणीकरण मांग रही है
- क्या आपने उस लेन-देन को अनुमति दी है

पहले स्कैन न करें और बाद में सवाल न पूछें।

3. बायोमेट्रिक डेटा देने से पहले ऑपरेटर की स्क्रीन देखें

जहाँ लेन-देन की जानकारी स्क्रीन पर दिखाई देती है, वहाँ उंगली रखने से पहले ऑपरेटर या डिवाइस की स्क्रीन देखें। सुनिश्चित करें कि दिखाई गई जानकारी उसी सेवा से संबंधित है जिसे आपने माँगा है।

यदि स्क्रीन पर अलग ग्राहक, अलग लेन-देन, अलग सेवा या अलग उद्देश्य दिखाई दे, तो स्कैनर पर उंगली न रखें।

4. केवल उसी लेन-देन के लिए बायोमेट्रिक डेटा दें जिसे आपने स्वीकृत किया है

एक स्वीकृत लेन-देन का अर्थ है केवल उसी उद्देश्य के लिए बायोमेट्रिक कैप्चर। असंबंधित कार्य के लिए अतिरिक्त कैप्चर न दें। यदि दोबारा कैप्चर माँगा जाए, तो पूछें: “मेरा बायोमेट्रिक डेटा फिर से क्यों आवश्यक है?”

5. हर बायोमेट्रिक प्रयास के बाद परिणाम की पुष्टि करें

उंगली रखने के बाद देखें कि प्रमाणीकरण:

- सफल हुआ
- विफल हुआ
- रद्द हुआ
- अभी लंबित है

पिछले प्रयास का परिणाम जाने बिना तुरंत दोबारा उंगली न रखें।

6. बार-बार बायोमेट्रिक प्रयास माँगे जाने पर सतर्क रहें

उंगली की स्थिति, सेंसर की गुणवत्ता, कनेक्टिविटी या अन्य कारणों से कभी-कभी वास्तविक बायोमेट्रिक कैप्चर विफल हो सकता है। लेकिन यदि ऑपरेटर बार-बार स्कैन करने को कहे, तो:

रुकें → स्क्रीन देखें → कारण पूछें → पिछले परिणाम की पुष्टि करें

हर पुनः प्रयास की आवश्यकता समझे बिना लगातार बायोमेट्रिक कैप्चर न दें।

7. अपने बायोमेट्रिक डेटा पर अपना नियंत्रण बनाए रखें

प्रमाणीकरण के दौरान आपकी उंगली आपके ही नियंत्रण और निगरानी में रहनी चाहिए। स्कैनर पर उंगली स्वयं रखें। किसी व्यक्ति को बिना लेन-देन समझाए आपकी उंगली बार-बार दबाने, रखने या उपयोग करने की अनुमति न दें।

8. केवल वास्तविक और स्वीकृत बायोमेट्रिक स्कैनर का उपयोग करें

आधार प्रमाणीकरण के लिए अपना बायोमेट्रिक डेटा केवल अधिकृत प्रमाणीकरण प्रक्रिया और स्वीकृत बायोमेट्रिक डिवाइस के माध्यम से दें।

इनसे जुड़े अज्ञात डिवाइस पर संदेह करें:

- व्यक्तिगत लैपटॉप
- अप्रमाणित मोबाइल फोन
- अज्ञात एप्लिकेशन
- अनधिकृत वेबसाइट
- अपरिचित POS टर्मिनल
-

9. प्रमाणीकरण से पहले उंगली साफ रखें

साफ और सामान्य रूप से सूखी उंगली का उपयोग करें। धूल, अधिक नमी, ग्रीस या गंदगी वास्तविक प्रमाणीकरण को विफल कर सकती है और अनावश्यक बार-बार स्कैन की स्थिति पैदा कर सकती है।

10. बायोमेट्रिक कैप्चर को स्वयं देखते रहें

पूरी प्रमाणीकरण प्रक्रिया के दौरान उपस्थित रहें और देखें: लेन-देन चयन → बायोमेट्रिक कैप्चर → परिणाम। ऑपरेटर द्वारा एप्लिकेशन, लेन-देन या ग्राहक विवरण बदलते समय ध्यान न हटाएँ।

11. अपने आधार प्रमाणीकरण इतिहास की समय-समय पर समीक्षा करें

आधिकारिक आधार सेवाओं के माध्यम से अपना Aadhaar Authentication History समय-समय पर जाँचें। इनमें विशेष रूप से देखें:

- ऐसे प्रमाणीकरण जिन्हें आप पहचानते नहीं हैं
- अनपेक्षित बायोमेट्रिक लेन-देन
- असामान्य तारीख या समय
- अज्ञात अनुरोध करने वाली संस्था
- बार-बार विफल प्रमाणीकरण

यदि कोई ऐसा लेन-देन मिले जो आपने नहीं किया, तो उसकी तुरंत जाँच करें और उपलब्ध प्रमाण के साथ संबंधित प्राधिकरण को रिपोर्ट करें।

12. संदिग्ध गतिविधि के बाद तुरंत अपने बायोमेट्रिक्स लॉक करें

यदि आपको लगे कि आपके बायोमेट्रिक डेटा का गलत उपयोग हुआ है या कोई अज्ञात प्रमाणीकरण हुआ है, तो अपने आधार बायोमेट्रिक्स को तुरंत लॉक करें। इसके बाद प्रमाणीकरण इतिहास देखें और उपयुक्त आधिकारिक माध्यम से संदिग्ध लेन-देन की रिपोर्ट करें।

कैसे करें, यह जानने के लिए वीडियो देखें: <https://www.youtube.com/shorts/WQ47pAoFu74>

13. अपने पंजीकृत मोबाइल नंबर को सुरक्षित रखें

आधार सेवाओं के नियंत्रण में आपका पंजीकृत मोबाइल नंबर महत्वपूर्ण भूमिका निभाता है। अपने फोन, SIM, OTP और आधार खाते की पहुँच को सुरक्षित रखें।

14. जहाँ उचित हो, Virtual ID का उपयोग करें

जहाँ सेवा इसका समर्थन करती है, वहाँ अनावश्यक रूप से आधार नंबर साझा करने के बजाय Aadhaar Virtual ID का उपयोग करने पर विचार करें।

15. सहमति देने से पहले उद्देश्य पूछें

बायोमेट्रिक डेटा देना बिना जाँच के नियमित आदत नहीं बननी चाहिए। प्रमाणीकरण से पहले जानें: कौन मांग रहा है → क्यों आवश्यक है → किस लेन-देन को अनुमति दी जा रही है।

क्या न करें - इन कार्यों से हमेशा बचें

1. डिजिटल प्रमाणीकरण के लिए अपने बायोमेट्रिक डेटा को कागज पर न दें या उसकी प्रतिकृति न बनाएँ

आधार या सामान्य इलेक्ट्रॉनिक बायोमेट्रिक प्रमाणीकरण के लिए बायोमेट्रिक डेटा की अलग भौतिक प्रति या प्रतिरूप बनाने की आवश्यकता नहीं होनी चाहिए।

बिना आवश्यक अधिकृत कारण के अपने अंगूठे का निशान या अन्य बायोमेट्रिक प्रतिरूप इन पर न दें:

- खाली कागज
- ढीले पत्रे
- कार्ड
- लेबल

ऐसे फॉर्म जो किसी अधिकृत आवश्यकता से संबंधित न हों

बायोमेट्रिक निशान या उसका भौतिक प्रतिरूप संवेदनशील बायोमेट्रिक जानकारी को उजागर कर सकता है।

2. किसी सामग्री का उपयोग करके अपने बायोमेट्रिक डेटा की प्रतिकृति न बनाएँ

किसी भी सामग्री से बायोमेट्रिक डेटा की कॉपी, छाप या प्रतिरूप न बनाएँ। आपका बायोमेट्रिक डेटा अधिकृत बायोमेट्रिक डिवाइस से लाइव कैप्चर होना चाहिए, किसी वस्तु या संग्रहित प्रतिरूप के रूप में नहीं।

3. किसी को अपने बायोमेट्रिक डेटा की कॉपी बनाने की अनुमति न दें

किसी ऐसे व्यक्ति के साथ सहयोग न करें जो आपसे निम्न कार्य करने को कहे:

- बायोमेट्रिक मोल्ड या प्रतिकृति बनाना
- आपके बायोमेट्रिक पैटर्न की कॉपी बनाना
- “टेस्टिंग” के लिए नमूना देना
- उंगली को किसी असामान्य सामग्री पर दबाना
- अनधिकृत डिवाइस टेस्टिंग के लिए बायोमेट्रिक निशान या नमूना देना

केवल तभी ऐसा करें जब यह स्पष्ट रूप से अधिकृत कानूनी या आधिकारिक प्रक्रिया का हिस्सा हो।

4. अपने बायोमेट्रिक डेटा को इमेज के रूप में संग्रहित न करें

जानबूझकर अपने बायोमेट्रिक डेटा की फोटो, स्कैन या फ़ाइल बनाकर JPG, PNG, PDF, स्क्रीनशॉट, स्कैन किए गए दस्तावेज़, मोबाइल इमेज या कंप्यूटर फ़ाइल के रूप में न रखें। आपकी बायोमेट्रिक पहचान को सामान्य फोटो की तरह नहीं माना जाना चाहिए।

5. अपने फोन की गैलरी में बायोमेट्रिक डेटा की इमेज न रखें

फिंगरप्रिंट, आइरिस, चेहरे या अन्य बायोमेट्रिक कैप्चर की स्पष्ट इमेज को गैलरी, डाउनलोड, नोट्स, फ़ाइल मैनेजर, ईमेल या क्लाउड ड्राइव में रखने से बचें।

6. WhatsApp या अन्य मैसेजिंग ऐप से बायोमेट्रिक डेटा न भेजें

बायोमेट्रिक निशान, इमेज या कैप्चर फ़ाइल को WhatsApp, Telegram, ईमेल, SMS/MMS, सोशल मीडिया या चैट एप्लिकेशन के माध्यम से न भेजें। वास्तविक बायोमेट्रिक प्रमाणीकरण के लिए किसी को आपके बायोमेट्रिक डेटा की फोटो, इमेज या फ़ाइल भेजना आवश्यक नहीं होना चाहिए।

7. अज्ञात वेबसाइट या ऐप पर बायोमेट्रिक डेटा अपलोड न करें

“वेरिफिकेशन” के नाम पर किसी अज्ञात वेबसाइट, मोबाइल एप्लिकेशन, रजिस्ट्रेशन फॉर्म या टेस्टिंग पोर्टल पर बायोमेट्रिक इमेज या डेटा फ़ाइल अपलोड न करें।

8. किसी को अपने बायोमेट्रिक डेटा की फोटो या कॉपी बनाने की अनुमति न दें

वैध और स्पष्ट रूप से बताए गए कारण के बिना किसी ऑपरेटर या अन्य व्यक्ति को आपके अंगूठे के निशान, कागज या सामग्री पर बने बायोमेट्रिक निशान, स्क्रीन पर दिख रहे कैप्चर या बायोमेट्रिक इमेज की फोटो लेने की अनुमति न दें।

9. अपनी उंगलियों की उच्च-रिज़ॉल्यूशन क्लोज़-अप तस्वीरें साझा न करें

ऐसी उच्च-रिज़ॉल्यूशन तस्वीरें जानबूझकर सार्वजनिक न करें जिनमें फिंगरप्रिंट की रेखाएँ, आइरिस विवरण, चेहरे की ज्यामिति या अन्य बायोमेट्रिक पहचान विशेषताएँ स्पष्ट दिखाई दें। अपने बायोमेट्रिक गुणों को अन्य संवेदनशील पहचान प्रमाणों जितनी ही सुरक्षा दें।

10. उद्देश्य जाने बिना अपना बायोमेट्रिक डेटा न दें

यदि कोई कहे, “बस यहाँ उंगली रखिए”, तो पहले पूछें कि कौन-सा लेन-देन किया जा रहा है। केवल इसलिए प्रमाणीकरण न करें क्योंकि आपके सामने स्कैनर रखा गया है।

11. खाली या अज्ञात लेन-देन के लिए बायोमेट्रिक डेटा न दें

इन स्थितियों में प्रमाणीकरण न करें:

- कोई लेन-देन दिखाई न दे
- ऑपरेटर उद्देश्य न समझा सके
- ग्राहक का विवरण गलत हो
- राशि या सेवा गलत हो
- किसी अन्य व्यक्ति का विवरण दिखाई दे
- एप्लिकेशन संदिग्ध लगे

12. कई बार विफल होने के बाद लगातार स्कैन न करें

क्या हो रहा है, यह जाँचे बिना लगातार बायोमेट्रिक कैप्चर देते न रहें। बार-बार विफलता के बाद:

रुकें → जाँचें → पूछें → पुष्टि करें

बार-बार स्कैन करना स्वचालित आदत न बनाएं।

13. लेन-देन पूरा होने के बाद ऑपरेटर को बायोमेट्रिक डेटा कैप्चर न करने दें

अधिकृत लेन-देन सफलतापूर्वक पूरा हो जाने के बाद दोबारा बायोमेट्रिक कैप्चर न दें, जब तक कि अलग वैध लेन-देन स्पष्ट रूप से समझाकर आपकी स्वीकृति न ली गई हो।

14. ध्यान भटका हुआ हो तो किसी को आपकी उंगली का उपयोग न करने दें

बायोमेट्रिक प्रमाणीकरण के दौरान सतर्क रहें। फोन कॉल पर बात करते समय, असंबंधित दस्तावेज़ पर हस्ताक्षर करते समय, स्क्रीन से ध्यान हटे होने पर या अन्य लेन-देन करते समय बायोमेट्रिक कैप्चर की अनुमति न दें।

15. स्कैनर पर उंगली रखकर न छोड़ें

केवल अधिकृत कैप्चर के लिए निर्देश मिलने पर उंगली रखें और कैप्चर पूरा होते ही हटा लें।

16. अज्ञात बायोमेट्रिक स्कैनर या कैप्चर डिवाइस का उपयोग न करें

केवल इस दावे पर किसी अज्ञात स्कैनर पर बायोमेट्रिक डेटा न दें कि वह आधार से जुड़ा है। केवल उसी सेवा के स्वीकृत प्रमाणीकरण सेटअप का उपयोग करें जिसे आप जानबूझकर इस्तेमाल कर रहे हैं।

17. अनधिकृत सॉफ्टवेयर से अपना बायोमेट्रिक डेटा कैप्चर न होने दें

इन माध्यमों से प्रमाणीकरण न करें:

- क्रैक किए गए एप्लिकेशन
- संशोधित सॉफ्टवेयर
- अज्ञात ब्राउज़र एक्सटेंशन
- अप्रमाणित बायोमेट्रिक एप्लिकेशन
- अनौपचारिक प्रमाणीकरण टूल

18. प्रमाणीकरण विफल होने पर उसे बायपास करने का प्रयास न करें

यदि वास्तविक प्रमाणीकरण विफल हो, तो किसी को भी स्कैनर में बदलाव करने, अनधिकृत एप्लिकेशन चलाने, बायोमेट्रिक डेटा में हेरफेर करने, संग्रहित बायोमेट्रिक इमेज/फ़ाइल या प्रतिकृति उपयोग करने, अथवा संदिग्ध तृतीय-पक्ष सॉफ्टवेयर चलाने की अनुमति न दें। अधिकृत सहायता से संपर्क करें या उपलब्ध होने पर स्वीकृत वैकल्पिक प्रमाणीकरण विधि का उपयोग करें।

19. अपना आधार OTP साझा न करें

बायोमेट्रिक प्रमाणीकरण करने वाले ऑपरेटर को आपके OTP तक अनियंत्रित पहुँच की आवश्यकता नहीं होती। OTP तभी साझा करें जब आप समझते हों कि वह किस विशिष्ट लेन-देन के लिए बना है और आपने उस लेन-देन को स्वीकृत किया है।

20. अपनी उंगली से किसी अन्य व्यक्ति को आपकी ओर से प्रमाणीकरण न करने दें

आपका बायोमेट्रिक डेटा आपकी पहचान का प्रतिनिधित्व करता है। किसी व्यक्ति को आपकी उंगली का उपयोग ऐसे लेन-देन की अनुमति देने के लिए न करने दें जिसे आपने स्वयं समझा और स्वीकृत न किया हो।

21. यह न मानें कि विफल स्कैन का अर्थ है “कुछ नहीं हुआ”

विफल बायोमेट्रिक प्रमाणीकरण भी एक प्रमाणीकरण प्रयास होता है। यदि बार-बार विफलता हो, तो बिना सोचे-समझे स्कैन जारी रखने के बजाय कारण की पुष्टि करें।

22. ऐसे आधार प्रमाणीकरण को नजरअंदाज न करें जिसे आप पहचानते नहीं हैं

यदि आपके प्रमाणीकरण इतिहास में कोई ऐसा लेन-देन दिखाई दे जो आपने शुरू नहीं किया था, तो उसे नजरअंदाज न करें। अपने बायोमेट्रिक्स लॉक करें और उस लेन-देन की जाँच करें।

इन चेतावनी संकेतों पर तुरंत रुकें

यदि कोई व्यक्ति निम्न में से कुछ करे, तो अपना बायोमेट्रिक डेटा न दें:

- यह न समझा सके कि आपका बायोमेट्रिक डेटा क्यों चाहिए
- लेन-देन दिखाने या समझाने से मना करे
- विफलता का कारण बताए बिना कई बार बायोमेट्रिक कैप्चर माँगे
- किसी दूसरी सामग्री पर बायोमेट्रिक निशान या प्रतिकृति बनाने को कहे
- आपके बायोमेट्रिक डेटा की फोटो या कॉपी लेना चाहे
- WhatsApp पर बायोमेट्रिक इमेज या फ़ाइल भेजने को कहे
- बायोमेट्रिक डेटा को JPG/PDF या अन्य फ़ाइल के रूप में सेव करना चाहे
- अज्ञात बायोमेट्रिक एप्लिकेशन का उपयोग करे
- स्कैनर को संदिग्ध सॉफ्टवेयर से जोड़े
- किसी अन्य व्यक्ति के लेन-देन को प्रमाणित करने को कहे
- आपका लेन-देन पूरा होने के बाद भी कैप्चर माँगे
- प्रमाणीकरण के दौरान आपका ध्यान भटकाने का प्रयास करे

यदि कई बार बायोमेट्रिक प्रयास हों - रुकें, जाँचें और पुष्टि करें

रुकें

लगातार अपना बायोमेट्रिक डेटा न दें।

जाँचें

ऑपरेटर या डिवाइस की स्क्रीन देखें और लेन-देन की पुष्टि करें।

पूछें

पिछला प्रमाणीकरण क्यों विफल हुआ, इसका कारण पूछें।

पुष्टि करें

सुनिश्चित करें कि दूसरा प्रमाणीकरण प्रयास वास्तव में आवश्यक है।

प्रमाणीकरण करें

संतुष्ट होने के बाद ही अपना बायोमेट्रिक डेटा दोबारा दें।

आधार बायोमेट्रिक सुरक्षा नियम

लॉक करें → अस्थायी रूप से अनलॉक करें → प्रमाणीकरण करें → फिर से लॉक करें

जब बायोमेट्रिक प्रमाणीकरण की आवश्यकता न हो, तो आधार बायोमेट्रिक्स लॉक रखें। जब आपको स्वयं प्रमाणीकरण करना हो, तभी उन्हें अस्थायी रूप से अनलॉक करें। आवश्यक प्रमाणीकरण पूरा होने के बाद अतिरिक्त सुरक्षा के लिए उन्हें फिर से लॉक करें।

कैसे करें, यह जानने के लिए वीडियो देखें: <https://www.youtube.com/shorts/WQ47pAoFu74>

याद रखें

आपका बायोमेट्रिक डेटा आपकी पहचान का हिस्सा है। इसे ऐसे संवेदनशील पहचान प्रमाण की तरह सुरक्षित रखें जिसे आसानी से बदला नहीं जा सकता।

- कभी इसकी कॉपी न बनाएं।
- कभी इसकी फोटो न लें।
- कभी इसे साझा न करें।
- कभी इसकी प्रतिकृति न बनाएँ।
- लेन-देन जाने बिना इसे कभी न दें।
- परिणाम जाँचे बिना लगातार स्कैन न करें।

इसे केवल वास्तविक, अधिकृत और स्पष्ट रूप से समझे गए लेन-देन के लिए उपयोग करें।