



CYBER SECURITY AWARENESS MONTH

CYBER SECURITY HANDBOOK 2026

A role-wise guide of Do's and Don'ts for State Cooperative Banks,
District Central Cooperative Banks and Regional Rural Banks

FOURTH EDITION · OCTOBER 2026



National Bank for Agriculture and Rural Development

Department of Supervision · CSITE
Head Office, Mumbai

Contents

	Foreword	3
1	Why Cyber Security Matters for Rural Cooperative Banks and Regional Rural Banks	4
2	Threat Landscape 2026	5
3	Branch Staff	6
4	Board and Senior Management	8
5	CISO and IT-in-charge	9
6	Vendors and Application Service Providers	10
7	Fraud Prevention and Mule Account Control	11
8	Incident Reporting - What, When and to Whom	12
9	Customer Protection and Grievance	13
10	Safe Use of Artificial Intelligence	14
11	Glossary	16

FROM THE CHIEF GENERAL MANAGER

Foreword



Cooperative banks and regional rural banks sit closest to the customer. A farmer taking a Kisan Credit Card loan, a self-help group collecting its monthly savings, a pensioner drawing cash at a micro-ATM - each of them trusts a branch that is often small, personal and known by name. That trust is the sector's greatest asset, and it is exactly what a cyber attacker sets out to exploit.

Over the past year, the pattern of attack has shifted. Fewer intrusions now begin with a technical breach of the bank. More of them begin with a person: a customer frightened into transferring money by a caller in uniform, a fingerprint captured on a fake device, an account opened at the counter without proper verification and used within days to move the proceeds of fraud. Artificial intelligence has made these approaches faster to produce and harder to spot.

This fourth edition is organised by role rather than by technical control. A branch clerk, an IT-in-charge, a Chief Executive Officer and a Board member each face different decisions, and each will find a section written for them. The format readers found useful in earlier editions has been retained: plain Do's and Don'ts, in short sentences.

Cyber security is not the responsibility of the IT department alone. It is exercised at the counter, in the Board room, in the vendor contract and in every conversation with a customer.

Sanjay Kumar Gupta

Chief General Manager
Department of Supervision, NABARD

01

THE STAKE

Why Cyber Security Matters for Rural Cooperative Banks and Regional Rural Banks



A cyber incident at a rural bank is not only a technology failure. It is a failure of the promise made to a depositor. The consequences run in four directions at once.

1.1 What is at stake

Area	What an incident costs the bank
Deposits	Direct loss through unauthorised transactions, and the cost of compensating customers where liability rests with the bank.
Trust	A single publicised incident can trigger withdrawals across a district. In a cooperative structure, confidence is local and travels fast.
Continuity	A ransomware attack on core banking or on a service provider can halt all branches at once, including collections and government benefit transfers.
Supervision	Adverse supervisory findings, restrictions on the roll-out of digital products, and delay in approvals for new services.

1.2 Why this sector is targeted

- Banking services are increasingly digital, while staff strength and specialist skills at smaller banks have not grown at the same pace.
- A large part of the technology stack - core banking, mobile banking, payment switching - is operated by application service providers. The attack surface therefore sits partly outside the bank.
- Customers include first-time digital users, who are more easily misled by an authentic-sounding call or message.
- Branches in semi-urban and rural locations handle high cash and AePS volumes, which attracts both external fraud and insider misuse.

None of this makes a smaller bank less defensible. It makes discipline in the basics - verification, access control, patching, logging and reporting - more valuable than expensive tools.

02

WHAT YOU ARE UP AGAINST

Threat Landscape 2026



The following are the methods most often seen against banks of this sector. Each is described in plain terms, followed by the single most useful defence.

Threat	How it works	The one control that helps most
Mule accounts	Accounts opened with weak verification are used to receive and move the proceeds of fraud, often within days of opening.	In-person verification at account opening, and monitoring of early transaction patterns.
Digital arrest and impersonation	Fraudsters pose as police or regulatory officials on video calls and frighten customers into transferring money.	Alert counter staff who question large, hurried or unusual withdrawals.
AePS and biometric misuse	Fingerprints captured on unauthorised devices are used for withdrawals at micro-ATMs.	Customer education on locking Aadhaar biometrics, and scrutiny of Bank Mitra transaction patterns.
SIM swap	A duplicate SIM is obtained in the customer's name, diverting the OTP to the fraudster.	Cooling-off controls on mobile number change and on transactions after such a change.
Phishing and fake KYC messages	Messages appearing to come from the bank direct customers to fake pages to collect credentials.	Clear, repeated communication that the bank never sends KYC or update links.
Deepfake voice and video	An AI-generated voice or video of a senior official instructs a payment or the sharing of credentials.	A rule that no payment or credential request is acted upon without confirmation on a second known channel.
Ransomware through service providers	The attacker enters through a vendor connection or an unpatched server and encrypts bank systems.	Controlled, time-bound and recorded vendor access, with offline and tested backups.
Insider and privileged misuse	A staff member or a vendor engineer uses legitimate access beyond their mandate.	Least privilege, unique user IDs and periodic review of privileged activity logs.
Look-alike websites and apps	A domain or an app closely resembling the bank's name is used to collect customer credentials.	Regular monitoring for look-alike domains and prompt take-down requests.

03

AT THE COUNTER
Branch Staff

This chapter is for branch managers, officers, clerks, cashiers, field staff and business correspondents. It covers what is done at the counter, in the field and on the branch systems.

3.1 At the Counter



✓ THINGS TO DO

✓ Verify in Person

See the customer, check the original documents and match the photograph. A photocopy or a scanned image is not verification.

✓ Check the Mobile Number

Before registering a mobile number, check whether the same number is already linked to other, unrelated accounts.

✓ Question Unusual Instructions

When a customer breaks a fixed deposit in a hurry, transfers a large sum to an unknown account, or is anxious and on the phone throughout, pause and ask a few gentle questions.

✓ Explain the Bank's Rules Aloud

Tell every new customer that the bank will never ask for an OTP, PIN or password, and never send a KYC link. Repetition is what makes this stick.

✓ Record What You Notice

If something at the counter appears irregular, put it in writing to the Branch Manager the same day. An oral mention leaves no trail.

✓ Keep the Counter Clear

Do not leave account opening forms, KYC papers or printouts of customer data on the counter or in open trays.

✓ Use the Local Language

Display and explain cyber safety messages in the language the customer actually speaks. Awareness in a language not understood is no awareness at all.

✗ DON'T DO IT

✗ Don't Open Accounts on Reference Alone

An introduction by a known person, an agent or a local representative does not replace verification. Repeated introductions by the same person are themselves a warning sign.

✗ Don't Rush Verification Under Pressure

Pressure to complete an account quickly - from the customer, an agent or within the bank - is exactly when mistakes are made.

✗ Don't Dismiss Dormant Accounts

Sudden activity in a dormant or small account is a common sign of mule use. Report it rather than assuming the customer has returned.

✗ Don't Discuss Customer Details Openly

Account balances, loan positions and KYC details are not to be discussed in front of other customers or shared in personal conversations.

✗ Don't Accept Documents That Look Altered

Mismatched fonts, tampered photographs, or addresses that do not match the supporting proof must be escalated, not accommodated.

✗ Don't Handle Fraud Complaints Casually

A customer reporting an unauthorised debit is working against the clock. Act at once and record the time of reporting.

03 Branch Staff *(continued)*

■ 3.2 On the Branch Systems



✔ THINGS TO DO

- ✔ **Use Your Own User ID**
Every entry made under your user ID is attributed to you. Use only the ID issued to you, and ask for your own if you do not have one.
- ✔ **Lock Your Screen**
Lock the screen every time you leave the desk, even for a minute. Make it a habit rather than a decision.
- ✔ **Change Passwords Promptly**
Change your password when it is first issued to you, when it is reset, and whenever you suspect anyone else has seen it.
- ✔ **Report Strange Behaviour of Systems**
Slow systems, unexpected pop-ups, files that will not open, or a printer producing unfamiliar output can be early signs of an attack. Report them the same day.
- ✔ **Verify Requests by Calling Back**
For any request for credentials, account details or payment - however senior the sender appears - call back on a number you already have.
- ✔ **Keep Bank Data on Bank Systems**
Customer data belongs in the bank's systems. Move it to a personal device or a personal email account for no reason whatsoever.

✖ DON'T DO IT

- ✖ **Don't Share Your Login**
Sharing a password with a colleague during a rush is still a breach, and the liability stays with you.
- ✖ **Don't Use Branch Systems for Personal Work**
Personal email, social media, downloads and streaming on branch systems introduce risk for no business benefit.
- ✖ **Don't Open Unexpected Attachments or Links**
An unexpected invoice, notice or update link is the most common way ransomware enters a branch.
- ✖ **Don't Scan Unknown QR Codes**
Scanning a QR code is a payment instruction, not a way to receive money. Treat every unknown code as a request to pay.
- ✖ **Don't Photograph Screens**
Photographing customer data or system screens and sharing it on messaging groups is a data breach, whatever the intention.
- ✖ **Don't Plug In Unknown Devices**
Pen drives, external disks and charging cables from customers, vendors or visitors must not be connected to branch systems.
- ✖ **Don't Write Passwords Down**
Passwords on a note under the keyboard, inside a drawer or in a register defeat every other control in this handbook.

04

ACCOUNTABILITY

Board and Senior Management



This chapter is for the Board of Directors, the Chief Executive Officer or General Manager, and committees charged with risk and audit. The Board is accountable for the bank's cyber security posture; that accountability cannot be delegated to the IT department or to a vendor.

4.1 Governance and Oversight



✓ THINGS TO DO

✓ Approve and Review the Policy

Approve a board-level cyber security policy, and review it at least once a year or whenever the bank adds a significant digital service.

✓ Keep Cyber on the Agenda

Make cyber risk a standing item at Board meetings, with a short, plain-language report rather than a technical annexure.

✓ Appoint a Named CISO or IT-in-charge

Designate an officer responsible for information security, in writing, with defined authority and a reporting line that is independent of IT operations where the bank's size allows.

✓ Ask for Status, Not Assurance

Ask how many audit, VAPT and inspection findings are open, how many are overdue, and who owns each. A statement that "everything is in order" is not a status report.

✓ Fund Security as Protection of Deposits

Provide a defined budget line for cyber security. Treat it as the cost of protecting deposits, not as discretionary IT spending.

✓ Review Fraud and Red-Flagged Accounts

Review suspected mule accounts, red-flagged accounts and fraud cases at senior level every month, with trend data by branch.

✓ Approve an AI Usage Policy

Decide, in writing, which artificial intelligence tools staff may use, for what purposes, and what data may never be entered into them.

✓ Rehearse the Response

Require at least one annual exercise simulating a major incident, and take part in it. The Board's own decisions are part of what is being tested.

✓ Prepare the Communication

Keep pre-approved messages ready for customers, staff, the regulator and the press, so that the bank is not drafting them during a crisis.

✗ DON'T DO IT

✗ Don't Treat Cyber Security as an IT Subject

It is a business risk affecting deposits, continuity and reputation. A Board that leaves it entirely to IT has not discharged its responsibility.

✗ Don't Accept Verbal Compliance

Ask for evidence - closure reports, test results, signed compliance certificates - rather than assurance in a meeting.

✗ Don't Defer Findings Indefinitely

A finding carried forward from one inspection to the next is a decision to accept the risk. Record it as such, with reasons, or close it.

✗ Don't Approve Digital Products Without a Security Review

Every new channel - mobile banking, UPI, internet banking - must be assessed and tested before launch, not after.

✗ Don't Depend Entirely on the Service Provider

The regulator holds the bank accountable. A vendor's certification is useful evidence, not a transfer of responsibility.

✗ Don't Leave the Post Vacant

Where the CISO or IT-in-charge leaves, appoint a successor or an interim officer immediately. A vacant post is an uncontrolled period.

05

THE CONTROLS

CISO and IT-in-charge



This chapter is for the officer responsible for information security and for those running the bank's IT operations, whether in-house or coordinated with a service provider.

5.1 Core Operational Controls



THINGS TO DO

- ✓ **Maintain a Complete Asset Inventory**
Record every server, endpoint, network device, application, cloud service and data store, with an owner named against each. What is not listed cannot be protected.
- ✓ **Patch on a Defined Cycle**
Apply security patches to operating systems, databases, applications and network devices on a published schedule, with a shorter track for critical vulnerabilities.
- ✓ **Enforce Least Privilege**
Give each user only the access the role requires. Review privileged accounts at least quarterly and remove what is no longer needed.
- ✓ **Apply Multi-Factor Authentication**
Require it for all administrative access, remote access and access to critical applications.
- ✓ **Retain Logs for 180 Days**
Maintain ICT logs for a rolling period of 180 days within India, including logs of systems operated by the service provider, and be able to produce them on demand.
- ✓ **Synchronise System Clocks**
Synchronise all ICT systems with the time servers of the National Informatics Centre or the National Physical Laboratory, so that logs can be correlated across systems.
- ✓ **Segment the Network**
Separate branch networks, the data centre, ATM and switch networks, and any guest access. Segmentation is what limits the spread of an attack.
- ✓ **Test Backups by Restoring Them**
Keep offline or immutable copies and restore from them periodically. A backup that has never been restored is an assumption.
- ✓ **Run VAPT and Close the Findings**
Conduct vulnerability assessment and penetration testing before every major release and periodically thereafter, and track closure with dates and owners.
- ✓ **Monitor for Look-alike Domains**
Watch for domains and mobile applications resembling the bank's name, and pursue take-down promptly.
- ✓ **Control AI Tool Usage Technically**
Publish the list of approved tools and enforce it - block unapproved AI sites and browser extensions, and apply controls that prevent sensitive data from leaving the network.

DON'T DO IT

- ✗ **Don't Run End-of-Life Systems**
Operating systems, databases and devices no longer supported by the supplier will not receive security fixes. Replace them or isolate them with compensating controls and a documented plan.
- ✗ **Don't Leave Default Credentials in Place**
Change default usernames and passwords on every device and application before it goes into production, including network equipment and cameras.
- ✗ **Don't Give Vendors Standing Remote Access**
Vendor access must be raised on request, restricted to the task, time-bound, supervised and recorded.
- ✗ **Don't Use Shared Administrative Accounts**
Shared IDs make it impossible to attribute an action to a person and defeat the purpose of logging.
- ✗ **Don't Store Sensitive Data Unencrypted**
Customer data, credentials and keys must be encrypted at rest and in transit. Test environments must not hold live customer data.
- ✗ **Don't Ignore Low-Priority Alerts**
Attacks often begin as a small, unexplained event. An unexplained alert is a finding, not noise.
- ✗ **Don't Delay Reporting While Investigating**
Reporting timelines run from the time the incident is noticed, not from the time its cause is established.
- ✗ **Don't Assume the Cloud Is Secure by Default**
Configuration, access control and logging in a cloud service remain the bank's responsibility.

06

OUTSOURCED, NOT TRANSFERRED

Vendors and Application Service Providers



Most banks in this sector depend on an application service provider for core banking, payments and digital channels. Outsourcing the activity does not outsource the accountability. This chapter is for the officers who select, contract with and supervise those providers.

6.1 Selection, Contract and Supervision



✓ THINGS TO DO

✓ Do Due Diligence Before Onboarding

Assess the provider's security practices, certifications, incident history, financial stability and the capacity to support the bank's size.

✓ Write Security into the Contract

Specify encryption standards, access controls, incident notification timelines, audit rights, log retention, data location, sub-contracting limits and exit obligations.

✓ Reserve the Right to Audit

Retain the right for the bank, its auditors, NABARD and the regulator to inspect the provider's systems and records relating to the bank.

✓ Require Prompt Breach Notification

Require the provider to inform the bank immediately on noticing any incident, in time for the bank to meet its own 6-hour reporting obligation.

✓ Insist on Log Access

Make it a contractual condition that logs relating to the bank are retained for 180 days within India and produced to the bank on demand.

✓ Classify Vendors by Risk

Tier providers by the sensitivity of the data they handle and the impact of their failure, and apply proportionate oversight.

✓ Review Compliance Annually

Obtain and examine independent assurance reports, closure status of findings, and the provider's own security posture at least once a year.

✓ Plan the Exit at the Start

Agree in advance how data will be returned or destroyed, in what format, and over what period, so that the bank is never locked in.

✓ Maintain a Current Vendor Register

Keep a register of all providers, the services they render, the access they hold and the risk tier assigned.

✗ DON'T DO IT

✗ Don't Assume a Large Vendor Is a Safe Vendor

Size and reputation are not evidence. Verify, and record what was verified.

✗ Don't Rely on a Self-Assessment Questionnaire Alone

Supplement it with independent audit reports or assessments.

✗ Don't Allow Undisclosed Sub-Contracting

Require prior written consent before any part of the service is passed to a further party.

✗ Don't Share Production Data for Testing

Provide masked or synthetic data for development and testing environments.

✗ Don't Treat Assessment as a One-Time Event

A provider's risk profile changes with its own acquisitions, staff changes and incidents.

✗ Don't Delay Offboarding

On expiry or termination, withdraw all access immediately and obtain written confirmation that bank data has been returned or destroyed.

✗ Don't Accept Deficient Compliance Silently

Where a provider does not meet the agreed standard, record it, escalate it and, where warranted, bring it to the notice of the supervisor.

07

THE ACCOUNT IS THE CHANNEL

Fraud Prevention and Mule Account Control



A mule account is an account used to receive and move the proceeds of fraud. The account holder may be a willing participant, or may have been recruited with the promise of a small commission, or may not know at all. For the bank, the consequence is the same: freeze notices, investigation, supervisory attention and reputational damage.

7.1 Detection and Control



✓ THINGS TO DO

✓ Watch the First Thirty Days

Most mule accounts reveal themselves early. Review new accounts that receive many credits from unrelated remitters soon after opening.

✓ Track Common Identifiers

Run periodic checks for the same mobile number, email address, address or introducer appearing across unrelated accounts.

✓ Define Early Warning Signals

Adopt a written list of early warning signals, with the action required against each, so that detection does not depend on individual judgement.

✓ Act on Freeze Requests Promptly

Handle law enforcement freeze and lien requests within the timelines prescribed, and maintain a register of them.

✓ Escalate Quickly

Route suspicion from the branch to the fraud monitoring or CISO function the same day, through a defined channel.

✓ Review Business Correspondent Activity

Examine AePS and micro-ATM transaction patterns of each Bank Mitra for unusual volumes, repeated customers or transactions outside normal hours.

✓ Train the Counter

Repeat mule account training at branch level at least twice a year, using recent, anonymised examples.

✗ DON'T DO IT

✗ Don't Treat a Freeze Notice as the End of the Matter

A freeze notice indicates a control failure at opening or in monitoring. Examine how the account was opened and who verified it.

✗ Don't Rely on Alerts Alone

Automated alerts miss patterns that a branch officer can see. Counter awareness and system monitoring work together.

✗ Don't Ignore Small-Value Patterns

Fraud proceeds are deliberately broken into small amounts to stay below thresholds.

✗ Don't Allow Undocumented Mobile Number Changes

A change of registered mobile number shortly after account opening is a recognised warning sign and must be documented and verified.

✗ Don't Close the Account and Move On

Preserve account opening documents, transaction records and correspondence. They will be required by investigators and by the supervisor.

08

THE CLOCK STARTS AT DETECTION

Incident Reporting - What, When and to Whom



Reporting timelines run from the moment an incident is noticed, not from the moment its cause is understood. Reporting and investigation proceed in parallel.

8.1 Handling an Incident



✓ THINGS TO DO

✓ Report First, Investigate Alongside

The clock starts at detection. A report filed late is a separate lapse, over and above the incident itself.

✓ Preserve Evidence

Disconnect the affected system from the network but keep it powered and untouched where forensic examination is likely. Preserve logs before they rotate.

✓ Record the Timeline

Note the time of detection, of each action taken and of each report filed. This record is the first thing an examiner will ask for.

✓ Keep a Single Point of Contact

Designate a Point of Contact for CERT-In and keep the details current. Route all external communication through one officer.

✓ Inform Staff Factually

Tell staff what has happened and what they must do. Silence produces rumour and unsafe improvisation.

✓ Complete the Root Cause Analysis

Establish what allowed the incident, fix that cause, and record the closure with dates and owners.

✗ DON'T DO IT

✗ Don't Wait for Certainty

A suspected incident is reportable. Waiting until the cause is confirmed will breach the timeline.

✗ Don't Wipe or Rebuild in Haste

Reformatting the affected machine destroys the evidence needed to establish what happened and what else was reached.

✗ Don't Handle It Informally

Telephone calls and messages without a written record leave the bank unable to demonstrate what it did and when.

✗ Don't Leave the Service Provider to Report

The obligation is the bank's. Obtain the provider's inputs, but file the report yourself.

✗ Don't Pay a Ransom Without Considering the Consequences

Payment carries legal and regulatory implications, does not assure recovery, and must involve the Board and the supervisor.

✗ Don't Close Without Learning

An incident closed without corrective action will recur. Feed every incident back into training and controls.

09

THE FIRST HOUR

Customer Protection and Grievance



The first hours after an unauthorised transaction decide whether the money can be recovered. Customer protection is therefore a matter of speed at the counter as much as of policy.

9.1 Serving the Customer



✓ THINGS TO DO

✓ Register the Complaint Immediately

Record the date and time of the customer's first report. Liability under the customer protection framework depends on it.

✓ Help the Customer Call 1930

Do not merely give the number. Help the customer place the call and register the complaint on the National Cyber Crime Reporting Portal.

✓ Enable Alerts for Every Account

Ensure SMS and, where available, email alerts are active for all transactions, and that the registered contact details are current.

✓ Publish the Escalation Path

Display, at every branch and on the website, the name and contact of the grievance officer and the escalation route.

✓ Educate at Every Opportunity

Use account opening, KCC renewal, SHG meetings and pension disbursement days to repeat the core messages in the local language.

✓ Explain the Customer's Liability Position

Tell the customer plainly what the framework provides, so that the customer's expectation is based on the rules and not on rumour.

✓ Escalate Internally Within the Day

Route the complaint to the fraud monitoring function the same day so that the beneficiary account can be flagged.

✗ DON'T DO IT

✗ Don't Ask the Customer to Come Back Tomorrow

Delay in reporting directly reduces the chance of recovery and can increase the customer's liability.

✗ Don't Blame the Customer

A customer who was deceived needs the complaint registered, not a lecture. Education comes afterwards.

✗ Don't Treat It as a Branch Matter Alone

Every unauthorised transaction complaint is also an input to the bank's fraud monitoring and to incident reporting.

✗ Don't Give Assurances You Cannot Keep

Do not promise recovery or a refund. State the process and the timelines provided by the framework.

✗ Don't Leave the Complaint Unrecorded

An oral complaint that is not entered in the system does not exist when the matter is examined later.

10

SMART TOOLS, SAFE HANDS

Safe Use of Artificial Intelligence



Artificial intelligence tools are now within reach of every staff member and every fraudster. This chapter covers both sides: using these tools safely, and defending against their use by others.

10.1 Using AI Tools in the Bank



✓ THINGS TO DO

✓ Publish an Approved List

State which tools may be used, by whom and for what purposes, and make the list easy to find.

✓ Draw a Clear Line on Data

Customer data, account numbers, identity numbers, credentials, audit reports, board notes and internal correspondence are never to be entered into a public AI tool.

✓ Check Every Output

AI-generated text can be confidently wrong. An officer remains responsible for anything issued in the bank's name.

✓ Enforce the Policy Technically

Block unapproved AI sites and browser extensions on bank systems, and apply controls that prevent sensitive data from leaving the network.

✓ Train Staff on the Reason

Explain that data entered into a public tool leaves the bank permanently. Staff follow a rule they understand.

✗ DON'T DO IT

✗ Don't Paste Bank Data to Save Time

A list of borrowers pasted into a chatbot is a data breach, whatever the intention behind it.

✗ Don't Install AI Extensions Freely

Browser extensions can read everything on the screen, including core banking sessions.

✗ Don't Issue AI Output Unchecked

Figures, references and regulatory citations produced by an AI tool must be verified before use.

✗ Don't Assume a Free Tool Is Private

Free services commonly retain input for their own purposes. Read what the service states before use, and prefer an approved tool.

10 Safe Use of Artificial Intelligence *(continued)*

10.2 Defending Against AI-Enabled Fraud



✓ THINGS TO DO

✓ **Confirm on a Second Channel**

Any instruction to make a payment, change bank details or share credentials must be confirmed on a separately known number, irrespective of who appears to be asking.

✓ **Assume Voice and Video Can Be Faked**

A familiar face or voice on a call is no longer proof of identity.

✓ **Watch for Polished Phishing**

Poor grammar is no longer a reliable clue. Judge a message by what it asks for, not by how well it is written.

✓ **Report Suspicious Contact**

Report attempted deepfake or impersonation contact even when no loss occurred, so that others can be warned.

✗ DON'T DO IT

✗ **Don't Act on Urgency Alone**

Urgency and secrecy together are the signature of impersonation fraud.

✗ **Don't Trust Caller Identity on the Screen**

A displayed number or name can be falsified.

✗ **Don't Rely on a Single Approver**

Large or unusual payments should require a second, independent confirmation.

11

PLAIN LANGUAGE

Glossary



Terms used in this handbook, explained without jargon.

AePS - Aadhaar Enabled Payment System - a facility that allows basic banking transactions using an Aadhaar number and a fingerprint, typically at a micro-ATM or through a Bank Mitra.

ASP - Application Service Provider - a firm that operates a bank's core banking or other applications on the bank's behalf.

CERT-In - Indian Computer Emergency Response Team - the national agency for responding to cyber security incidents.

CISO - Chief Information Security Officer - the officer responsible for the bank's information security.

Deepfake - A video, image or voice recording generated or altered by artificial intelligence so that a person appears to say or do something they did not.

Data leakage controls - Technical controls that prevent sensitive information from being copied or sent outside the bank's network.

Early Warning Signal - A defined indicator that an account or a borrower may be connected with fraud, requiring examination.

Least privilege - The principle that a user is given only the access needed for their role, and no more.

Log - An automatically generated record of activity on a system, used to establish what happened and when.

Multi-factor authentication - A login that requires two or more different proofs of identity, such as a password and a one-time code.

Mule account - A bank account used to receive and move the proceeds of fraud.

Phishing - A message designed to look genuine in order to obtain credentials, card details or money.

Ransomware - Malicious software that encrypts a bank's data and demands payment for its release.

Red Flagged Account - An account classified as requiring closer examination on the basis of early warning signals.

SIM swap - Obtaining a duplicate SIM card in a customer's name so that one-time passwords are received by the fraudster.

Social engineering - Persuading a person to do something unsafe - share a password, make a payment - rather than attacking a system directly.

VAPT - Vulnerability Assessment and Penetration Testing - a structured test to find and demonstrate weaknesses in systems.

Vishing - A fraudulent telephone call intended to obtain confidential information.

Disclaimer - This handbook is an awareness publication. It does not replace or modify any instruction issued to banks, which prevails in case of any difference. Banks are to comply with the instructions applicable to them as amended from time to time.