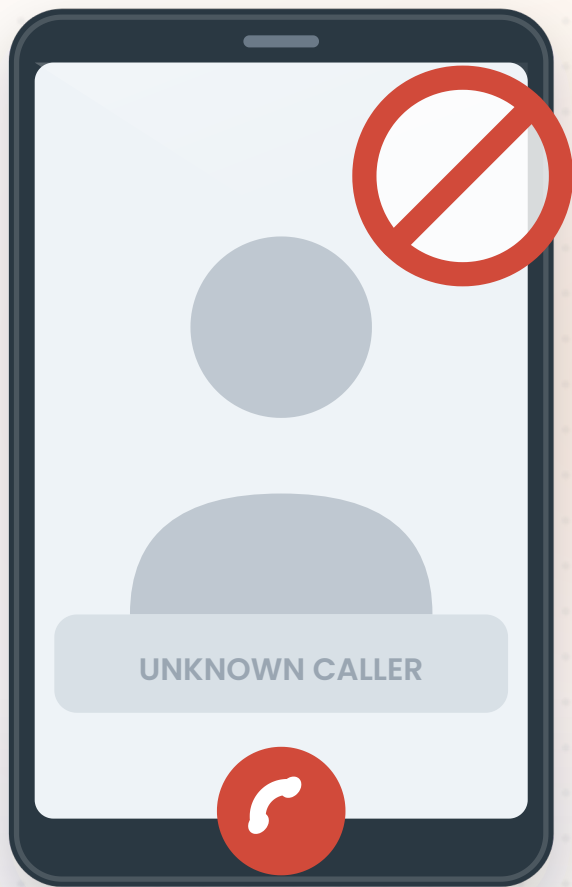


FOR CUSTOMERS

Police never arrest anyone on a video call



END THE CALL



Police, CBI or customs officials never question anyone on a video call.



No government office asks you to transfer money to "clear your name".



Nobody can order you to stay on a call or keep it secret from family.



Disconnect the call and tell a family member.

Hang up. Talk to family. Call 1930.

1930

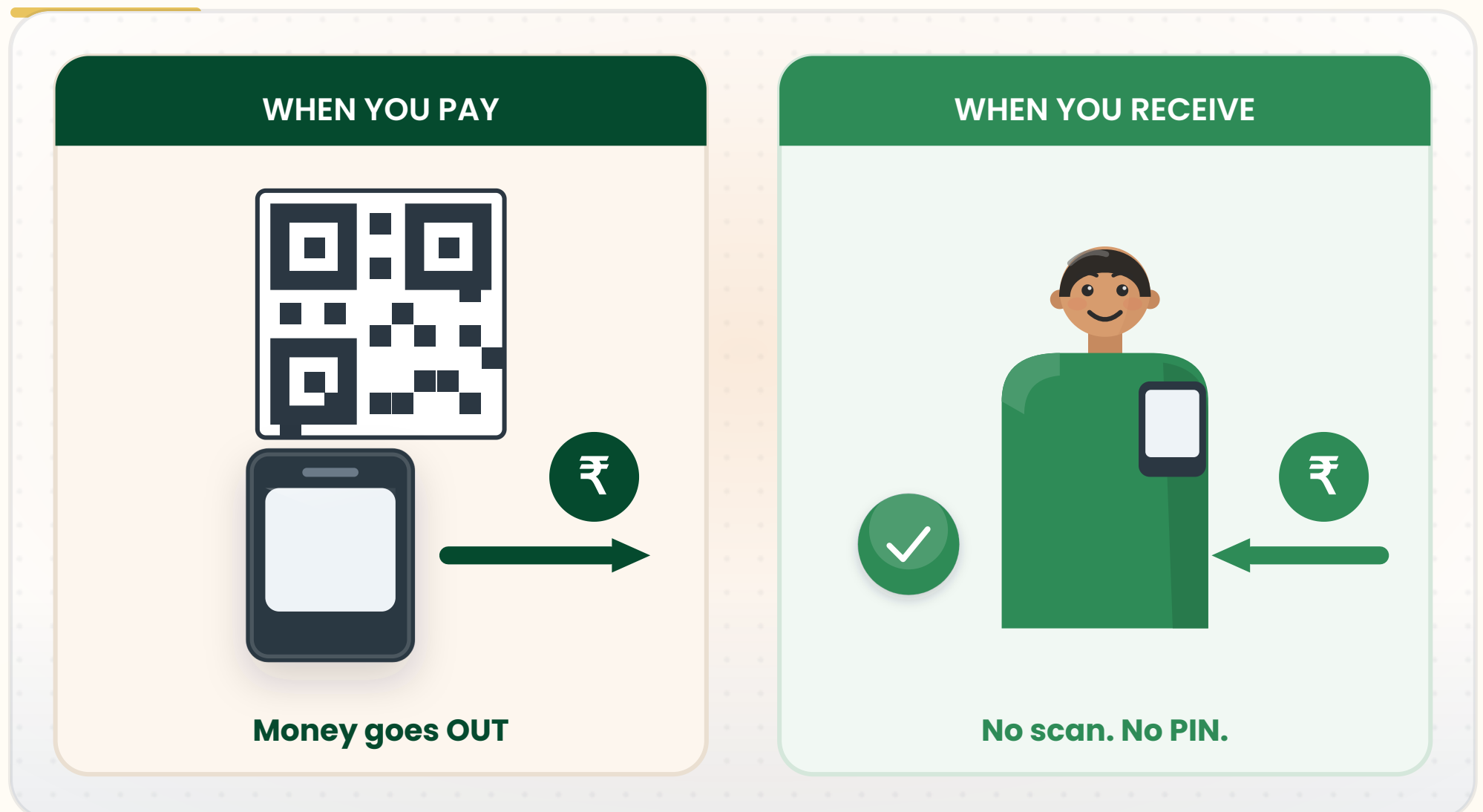
National Cyber Crime Helpline

Report online: www.cybercrime.gov.in
Contact your bank branch immediately



FOR CUSTOMERS

Scan a QR only to pay, never to receive



-  You never need to scan anything to receive money.
-  A QR code sent to you "for receiving payment" takes money out of your account.
-  Entering your payment PIN means money is leaving your account.
-  Check the name shown on the screen before you pay.

Receiving money? Don't scan. Don't enter your PIN.



CYBER SECURITY AWARENESS MONTH

OCTOBER 2026

FOR CUSTOMERS

Take your bank's number only from your bank



Numbers found through an internet search can be planted by fraudsters.



Real bank staff never ask you to install an app or share your screen.



Use the number printed on your passbook, on your card, or displayed at your branch.

Save your bank's real number in your phone today.

1930

National Cyber Crime Helpline

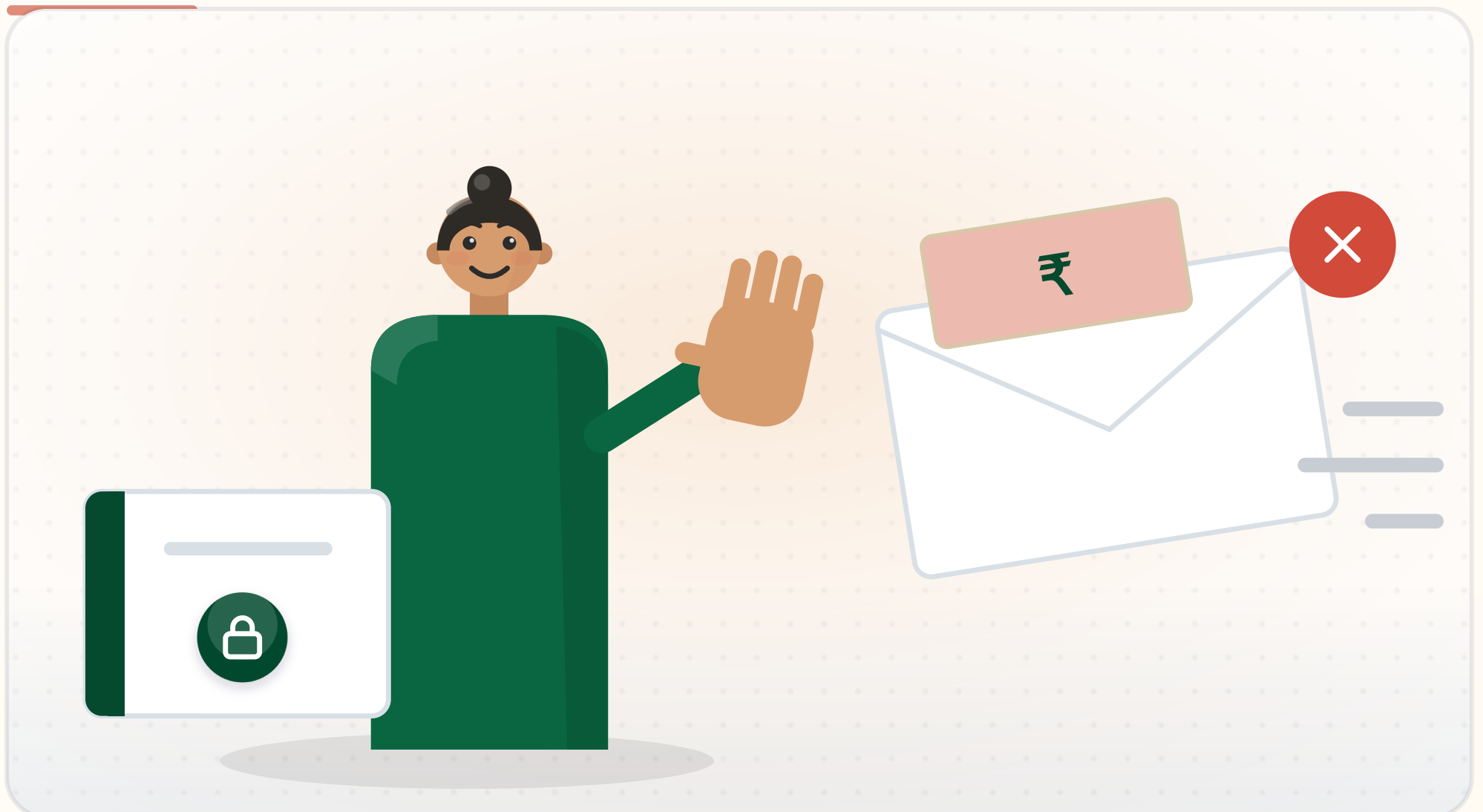
Report online: www.cybercrime.gov.in
Contact your bank branch immediately

Poster C3 · CSAM 2026 · NABARD · Department of Supervision, CSITE



FOR CUSTOMERS

Your bank account is not for rent



-  Strangers may offer you money to use your account, ATM card or cheque book.
-  The money passing through it may be stolen from other people.
-  Your account can be frozen and you may face legal action.
-  Never hand over your passbook, card or KYC papers to anyone for a fee.

Say no. Report such offers to your branch.



FOR CUSTOMERS

Cheated online? Act within the first hour



4 Save the proof

SMS, screenshots, ID

1 Call 1930

right away

3 File a complaint

on cybercrime.gov.in

2 Tell your branch

block card / account



Call 1930 immediately — the sooner you call, the better the chance of a hold.



Inform your branch to block your account or card.



Register a complaint on www.cybercrime.gov.in.



Keep screenshots, SMS messages and the transaction ID.

Save 1930 in your phone now, before you need it.

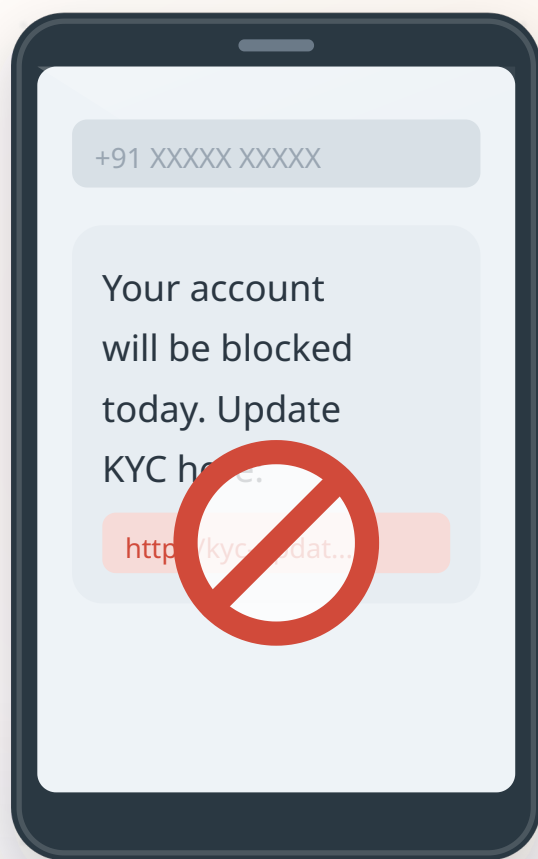
1930

National Cyber Crime Helpline

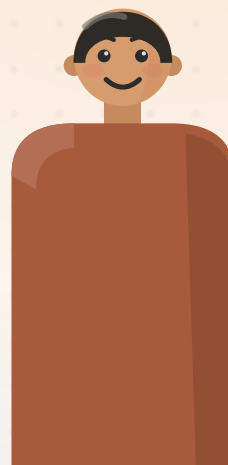
Report online: www.cybercrime.gov.in
Contact your bank branch immediately

FOR CUSTOMERS

No bank blocks an account by SMS



Don't click



Ask at your branch



A bank never sends a link to "update KYC" or "unblock" your account.



"Your account will be blocked today" is written to make you panic and hurry.



KYC is updated at the branch or by a verified bank officer — never through a link.



Unsure? Call the number on your passbook, not the number in the message.

Got such a message? Walk into your branch.

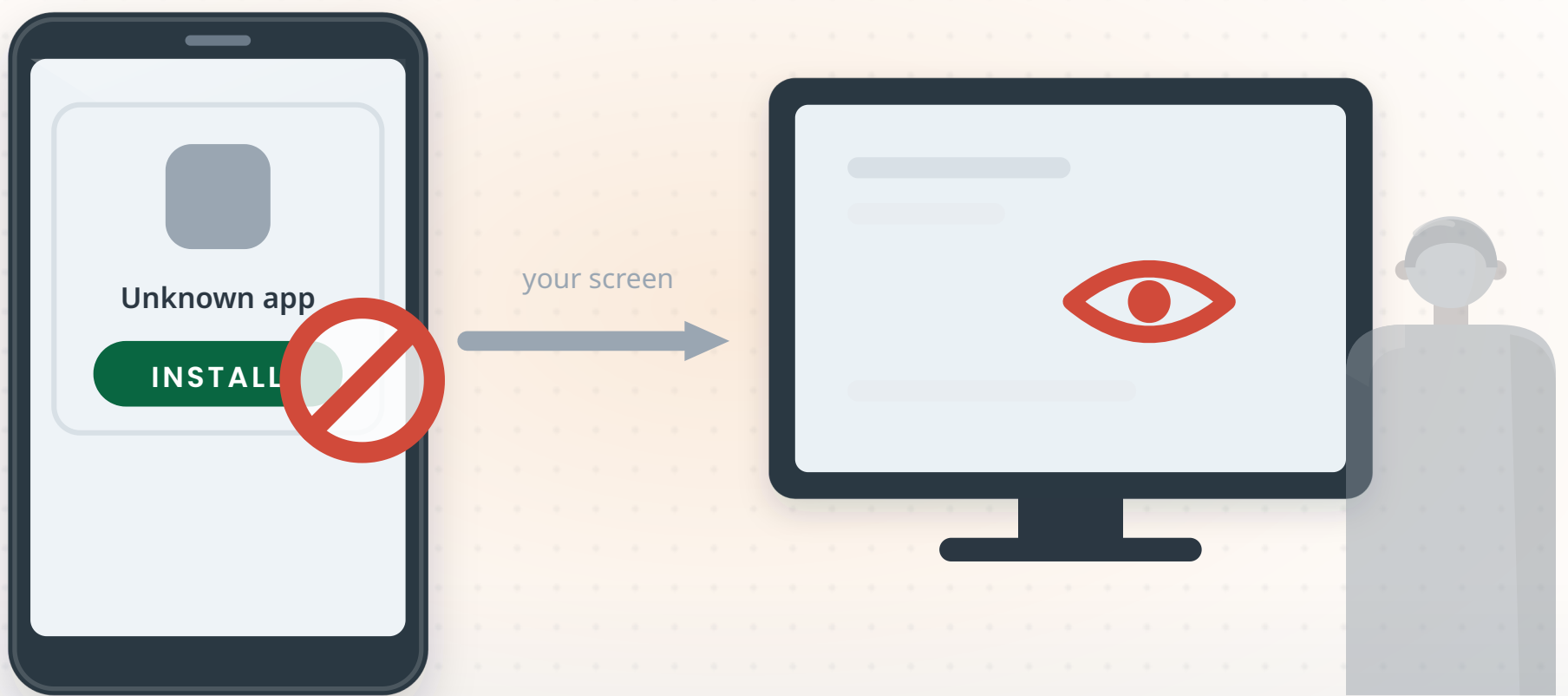
1930

National Cyber Crime Helpline

Report online: www.cybercrime.gov.in
Contact your bank branch immediately

FOR CUSTOMERS

Never install an app a caller asks you to



Never install

They see your OTP too



Screen-sharing and "support" apps let a stranger watch everything you type.



They will see your OTP, your PIN and your balance as you enter them.



No bank, no helpline and no officer needs to see your screen.



Install apps only from your phone's official app store, on your own decision.

Asked to install or share your screen? Hang up.

1930

National Cyber Crime Helpline

Report online: www.cybercrime.gov.in
Contact your bank branch immediately



FOR CUSTOMERS

Your thumb can withdraw your money



Locked when not in use



Your thumb is your signature

-  At a BC point, your fingerprint works like your signature on a withdrawal.
-  You can lock your Aadhaar biometrics and unlock them only when you need them.
-  Always take the printed receipt and check the amount before you leave.
-  Check your SMS alerts. Money out without your thumb? Tell the branch at once.

Ask your branch how to lock your biometrics.



FOR CUSTOMERS

No real subsidy asks you to pay first

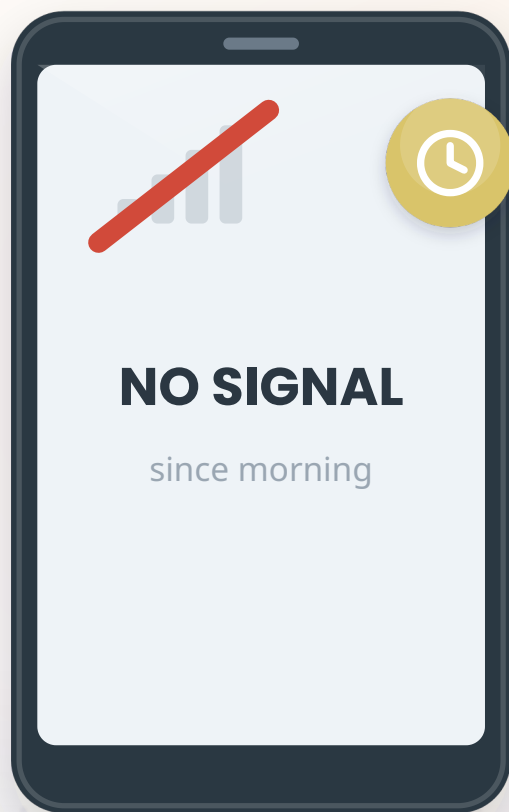
The illustration shows a digital message box on the left and a customer service counter on the right. The message box has a green header 'SUBSIDY APPROVED' and displays '₹ X,XX,XXX for you' with 'Claim before 5 pm today' below it. A red box with 'Pay ₹ 2,000 processing fee' is crossed out with a red prohibition sign. Below the message box, it says 'Fee first = fraud'. The counter on the right has a green checkmark icon, a person icon, and a button labeled 'ENQUIRY' with the text 'Check at your branch' below it.

- ₹ A genuine scheme never asks for a processing fee, a charge or a deposit.
- ⚠ "Claim before 5 pm today" is pressure, not a deadline.
- ⊘ A benefit is credited into your account. It is never collected from your account.
- 🏠 Check any scheme message at your branch before you pay anyone.

Pay nothing to receive money that is yours.

FOR CUSTOMERS

Phone dead for hours? Find out why



Hours with no network?



Your number,
their SIM

MOBILE OPERATOR



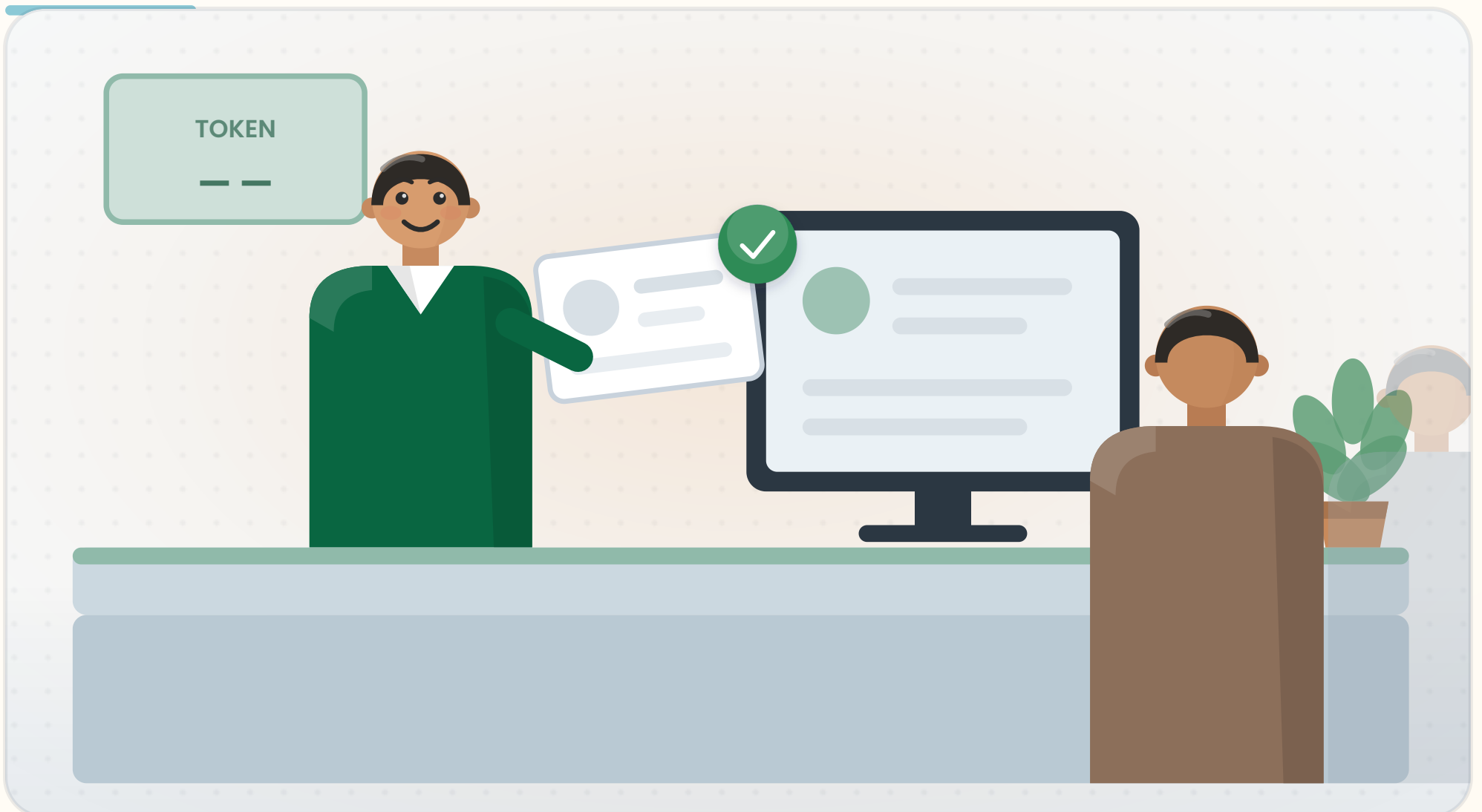
Then tell your bank

-  A sudden, long loss of signal can mean someone has taken over your number.
-  With your number they can receive your OTPs and reset your banking access.
-  Contact your mobile operator the same day and confirm no new SIM was issued.
-  Tell your branch so your account can be watched until it is settled.

No network for hours? Check with your operator today.

FOR BANK STAFF

Urgency at the counter? Slow down, verify.



-  Fraudsters pose as customers, relatives or "HO officials".
-  Check original ID and signature, not photocopies or photos on a phone.
-  Never change a mobile number or KYC detail on a telephone request.
-  Escalate doubtful requests to the Branch Manager.

Pressure is a warning sign. Verify every time.



FOR BANK STAFF

Your CBS login is your signature

YOUR SIGNATURE

CORE BANKING LOGIN

User ID

● ● ● ● ● ●

SIGN IN

🔒

One user. One login.

-  Every entry made under your user ID is recorded as yours.
-  Never share your user ID, password or OTP — not even with a senior.
-  Log off or lock the screen every time you leave your seat.
-  Going on leave? IT assigns access to your replacement. Do not hand over your password.

Your login, your responsibility. Keep it yours.

FOR BANK STAFF

Stop. Check. Then open that attachment.



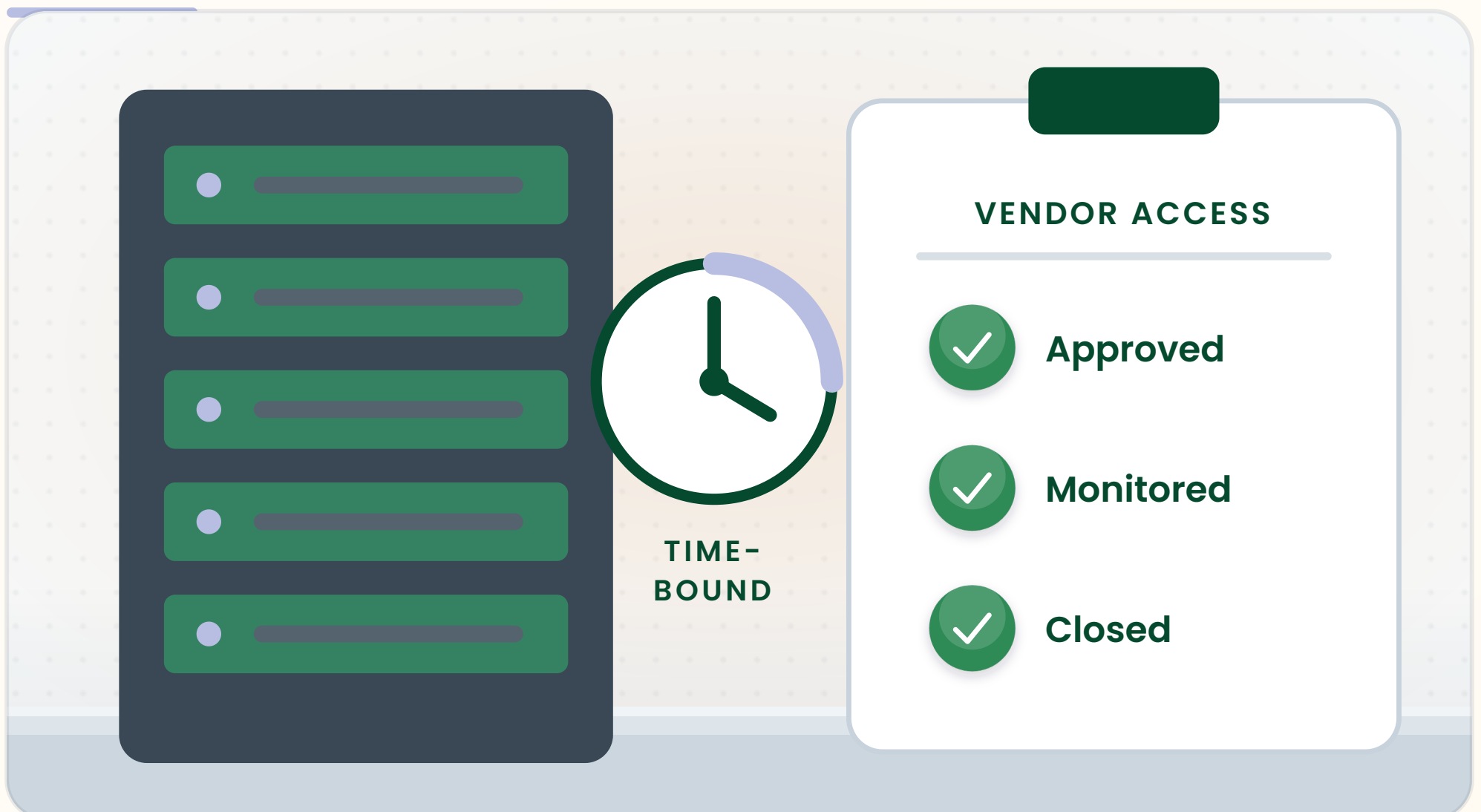
-  Ransomware usually enters through email attachments, links and pen drives.
-  Do not enable "macros" or "editing" on an unexpected document.
-  Files renamed or a ransom message on screen? Pull out the network cable — do not switch the PC off.
-  Inform the IT / CISO team at once. Never pay or contact the attacker.

Something odd on screen? Unplug and report first.



FOR IT STAFF & BRANCH MANAGERS

Vendor access: open for the task, closed after

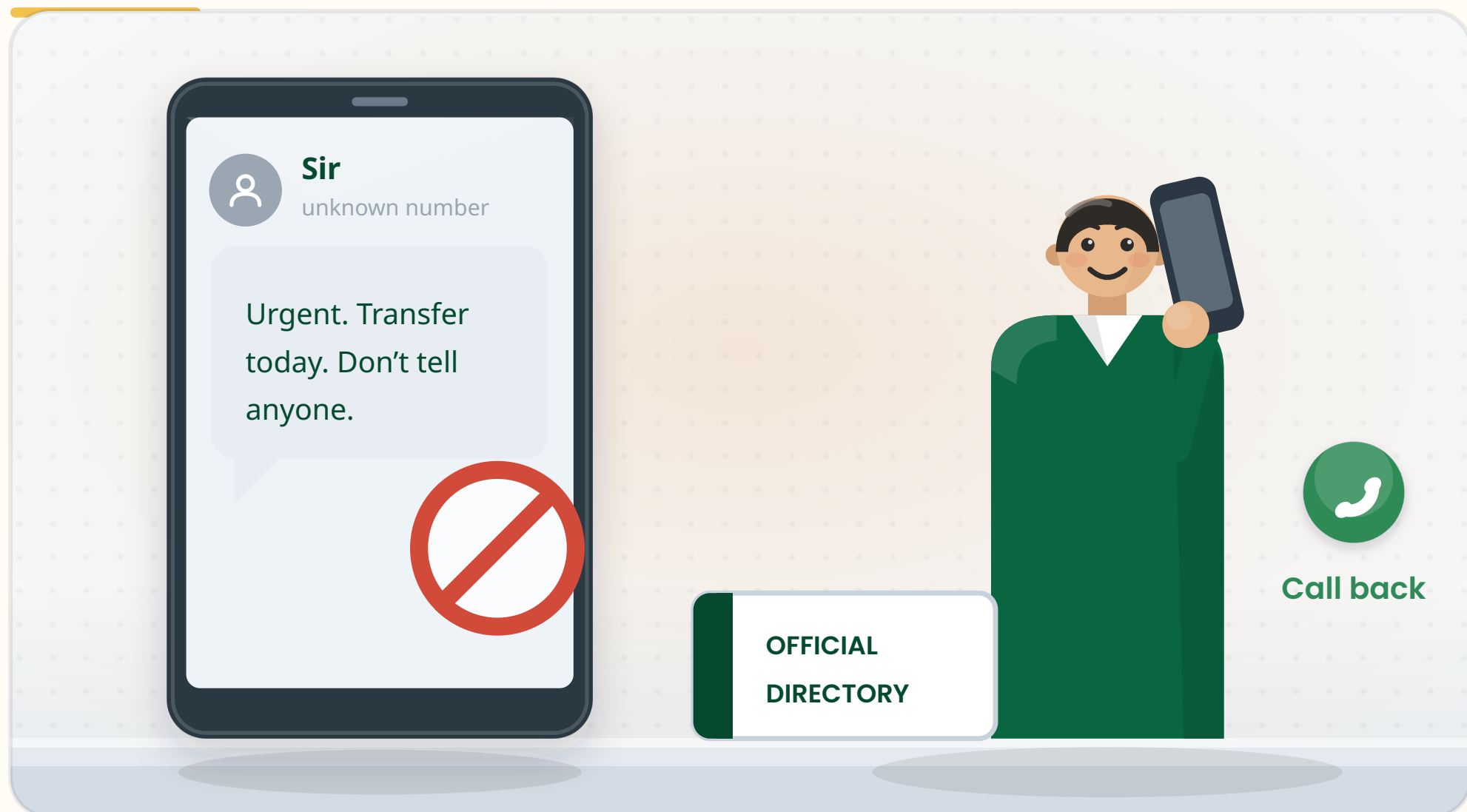


-  Give remote access only against an approved, time-bound request.
-  Monitor the session and record who accessed what, and when.
-  Never share administrator passwords over phone, email or chat.
-  Disable the access as soon as the work is done.

Approve. Watch. Close. Every time.

FOR BANK STAFF

Urgent transfer from "Sir"? Call back first.



Fraudsters copy the names and photos of senior officials on messaging apps and email.



The ask is usually an urgent fund transfer, a password or confidential data.



Verify on the known official number, not the number in the message.



Follow the approval process, no matter who is asking.

Genuine seniors welcome verification.

1930

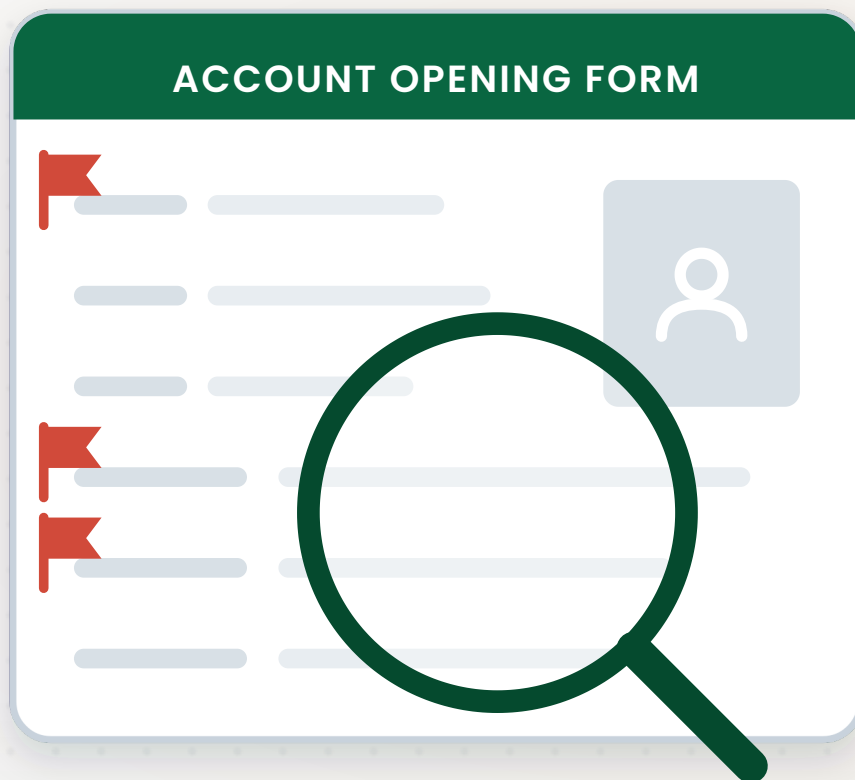
National Cyber Crime Helpline

Report online: www.cybercrime.gov.in
Contact your bank branch immediately



FOR BANK STAFF

A new account is a door. Know who walks in.



Same address? Same phone? Many accounts?



Watch for many accounts sharing one address, one phone number or one introducer.



Verify original documents and confirm the stated occupation and income fit.



A low-income account suddenly receiving and forwarding large sums is a red flag.



Raise such cases with the Branch Manager and the compliance desk without delay.

Open it right, and a mule account never opens.

1930

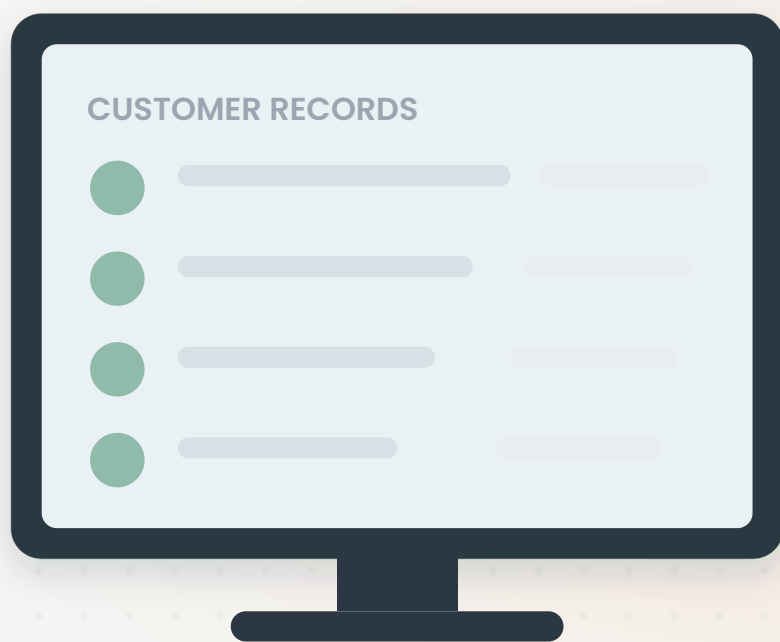
National Cyber Crime Helpline

Report online: www.cybercrime.gov.in
Contact your bank branch immediately



FOR BANK STAFF

Customer data stays inside the bank



No photos. No forwarding.



Stays inside the bank



Never photograph a screen or a document to send a detail to someone quickly.



Customer data does not travel on personal messaging apps or personal email.



Share records only through approved bank systems, with the approved people.



Collect printouts from the printer at once, and shred what is not needed.

Convenience is never a reason to move customer data.

1930

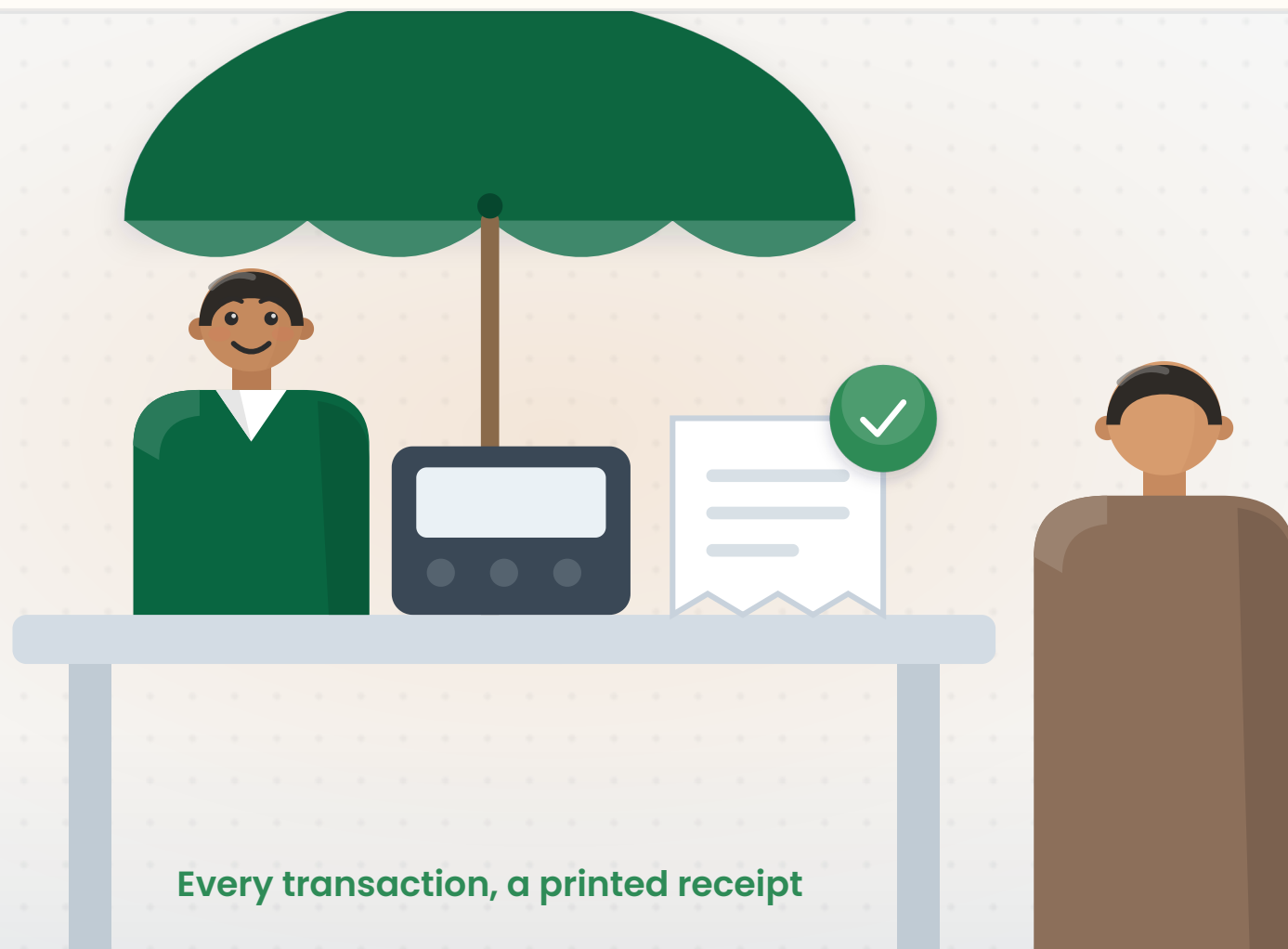
National Cyber Crime Helpline

Report online: www.cybercrime.gov.in
Contact your bank branch immediately



FOR BANK STAFF & BC AGENTS

The BC point is your branch too



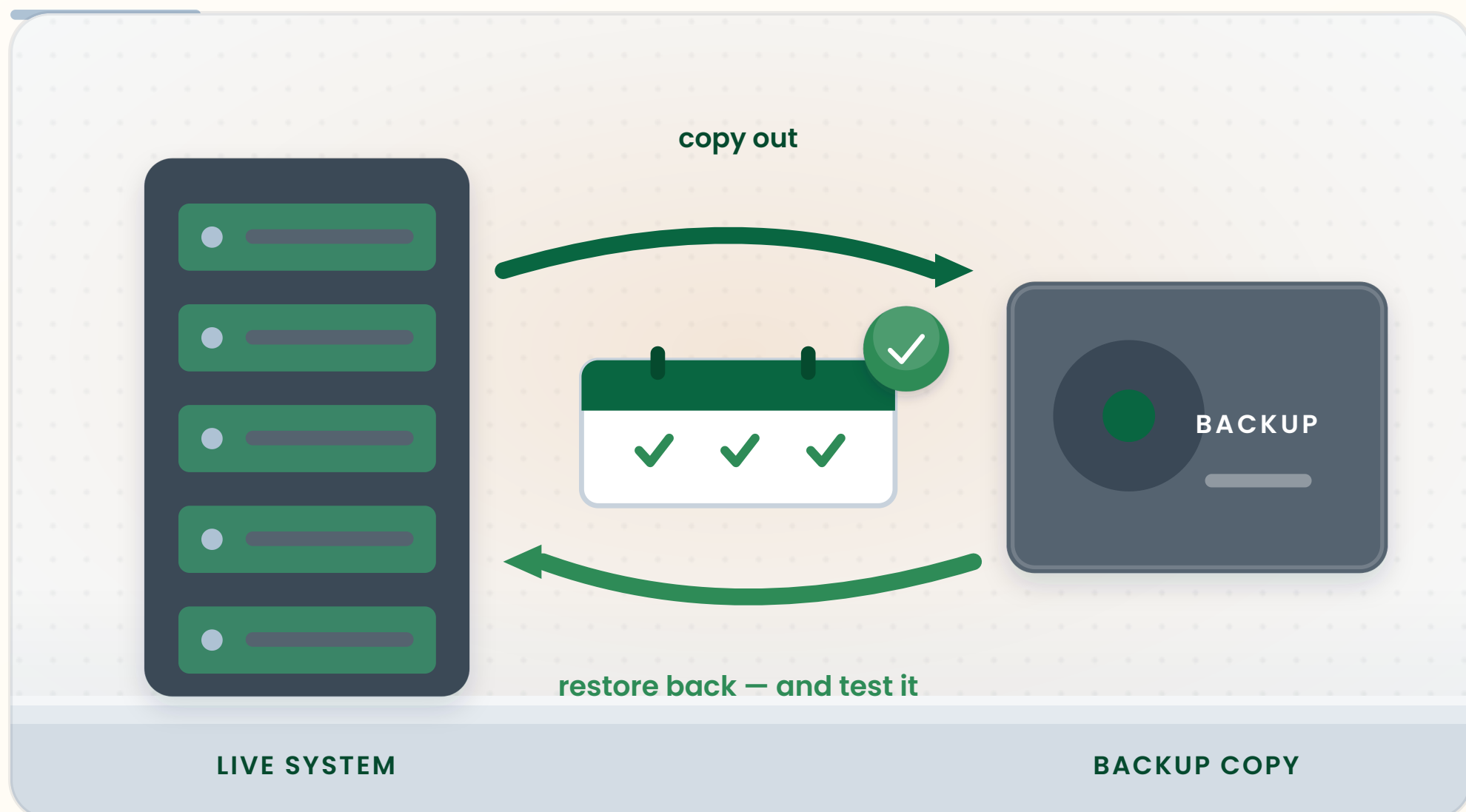
-  Hand over a printed receipt for every transaction, every time, unasked.
-  Never keep a customer's card, passbook, PIN or fingerprint for "later use".
-  Keep the device with you, updated and locked — never lend it to anyone.
-  Branches should check BC transaction reports and customer complaints regularly.

Same bank. Same duty. Same records.



FOR IT STAFF & MANAGEMENT

A backup you never restored is not a backup



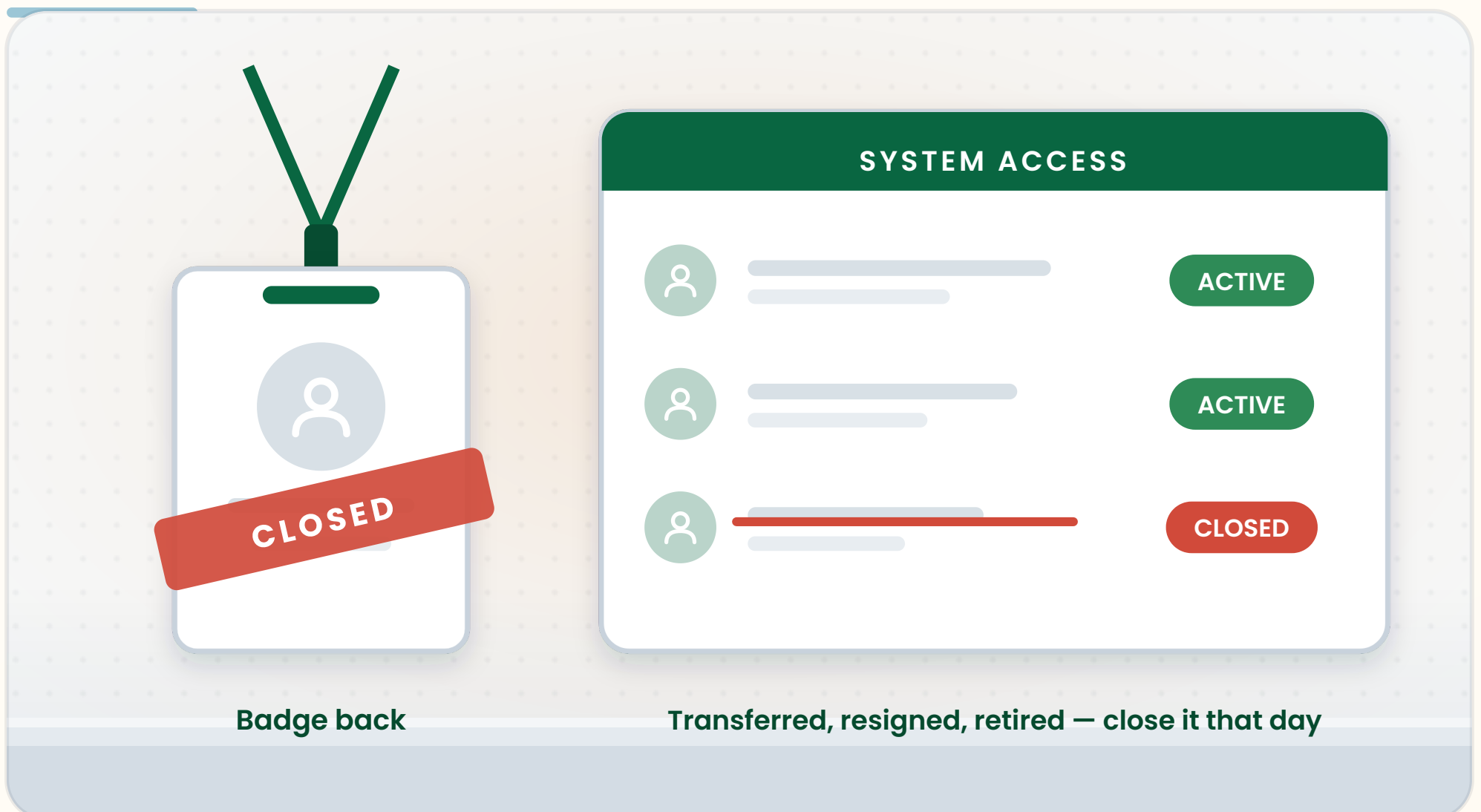
-  Test a real restore on a fixed schedule and write down how long it took.
-  Keep one copy offline or otherwise out of reach of the live network.
-  Check that the backup actually ran, and that it covered every critical system.
-  Record who tested it, what was restored and what failed — then fix what failed.

Test the restore before the day you need it.



FOR BANK STAFF & IT

Transferred or retired? Close the access that day



-  Leavers and transfers keep working access far longer than anyone expects.
-  Close the user ID, take back the token, the badge and the bank device the same day.
-  Review the full user list against the current staff list at fixed intervals.
-  A dormant live ID is an open door — and the entries will still carry that name.

Last working day means last working login.